802.11a/b/g Indoor Wireless Mesh Network Access Point

MAP-3100 / MAP-3120

Mesh Network Manager (MnM)

Management Utility User Manual

Copyright

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not PLANET, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, PLANET reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Revision

Mesh Network Manager User’s Manual for PLANET Wireless Mesh Access Point
Model: MAP-3100 / MAP-3120
Rev: 2.0 (February, 2008)
Part No. EM-MAP3K_MnMv2.doc

Table of Content

1 Overview

This document provides a details information and application guidance for the user of the management software, the PLANET Mesh Network Manager (MnM). This network management system is intended to perform an overall monitoring and configuring features for the PLANET Mesh Network.

2 System Requirement

The PLANET Mesh Network Manager is written in JAVA, hence it has the feature of cross platform, capable to run in most of the platform. The following are the recommended system requirement.

- 256 MB RAM (recommended minimum)
- 10 MB hard disk space
- Microsoft Windows 2000, XP (recommended)

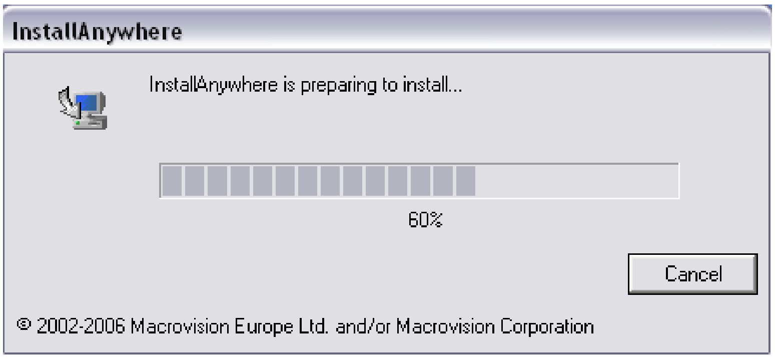
Besides, in order to enable the NMS to work properly, the following ports must be allowed through any firewall between the NMS and the agent:

- Port 161 (by default) – Use for standard SNMP Get and Set
- Port 162 (by default) – Use for listen to SNMP Trap
- Port 4608 (by default) – Used by the Discovery Tool
- Port 8188 (by default) – Use to listen for the Layer-2 node’s notification

3 Utility Installation and Un-installation

3.1 Installation

Insert the bundled CD into the CD-ROM drive to launch the auto run program. Once completed, a menu screen will appear. Click the “PLANET Mesh Network Manager” hyperlink and select “Open” or “Run” to initiate the install wizard.



InstallAnywhere

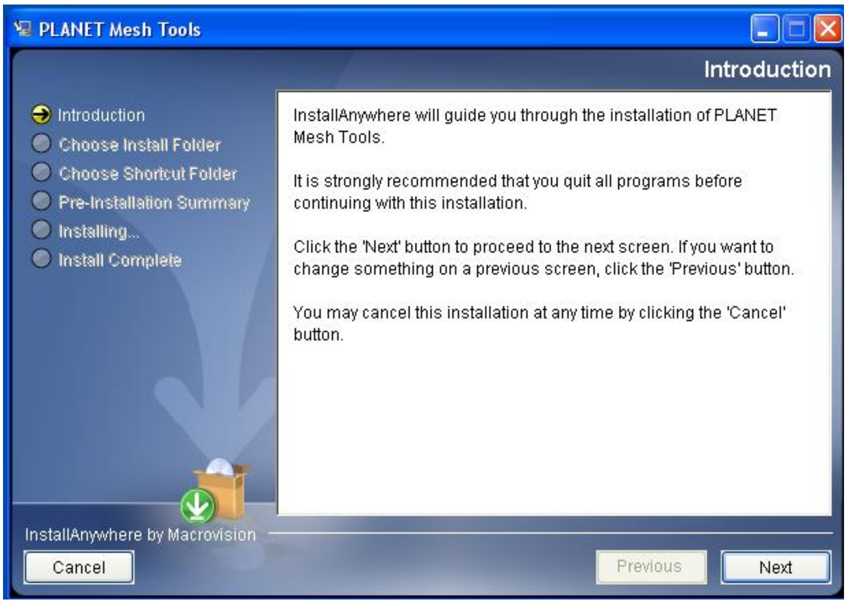
InstallAnywhere is preparing to install...

60%

© 2002-2006 Macrovision Europe Ltd. and/or Macrovision Corporation

After the wizard completes preparation, follow the 6 easy steps directed by the wizard to perform the installation.

3.1.1 Introduction



InstallAnywhere will guide you through the installation of PLANET Mesh Tools.

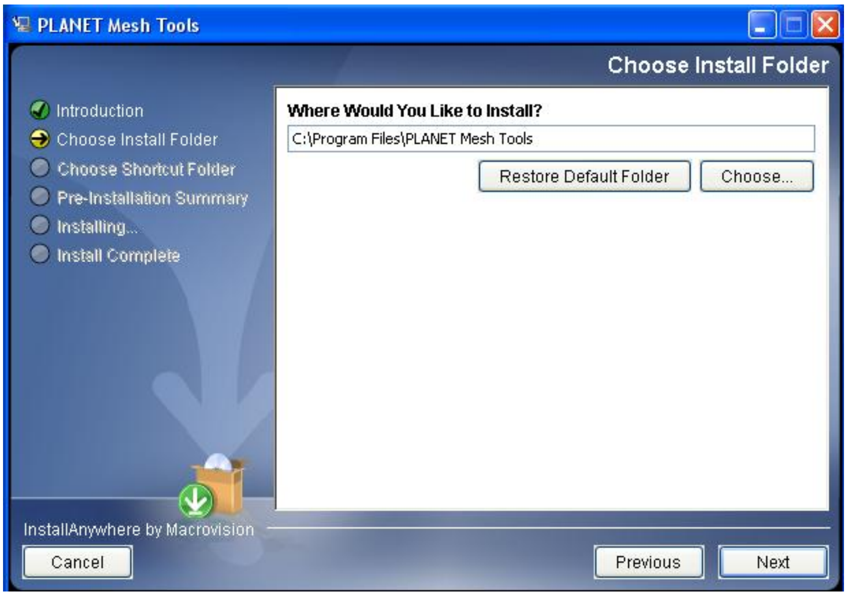
It is strongly recommended that you quit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

Simply explain what this software is about. Press **Next** to proceed.

3.1.2 Choose Install Folder

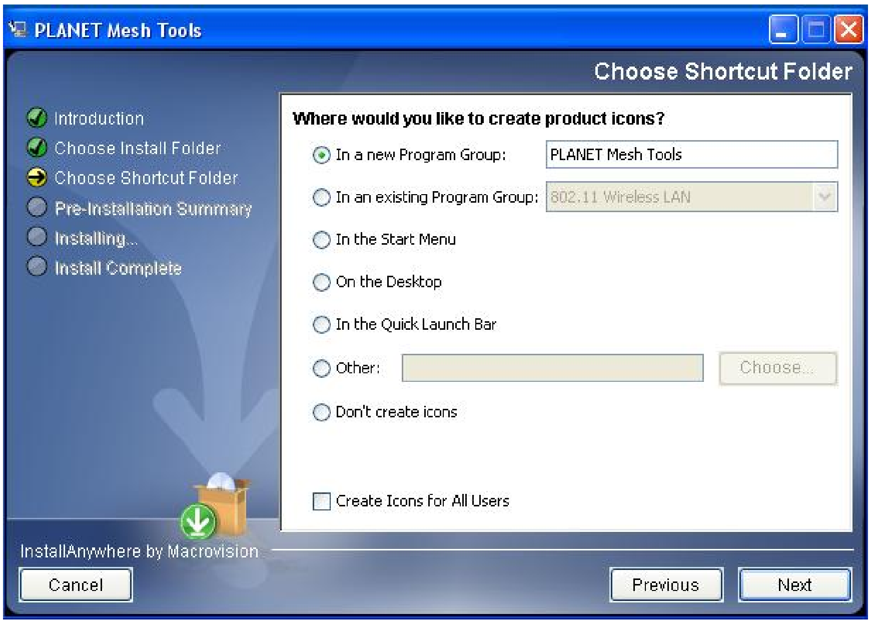


Where Would You Like to Install?

C:\Program Files\PLANET Mesh Tools

Prompt user to choose the install path (directory) and name the install folder. Press **Next** to proceed.

3.1.3 Choose Shortcut Folder



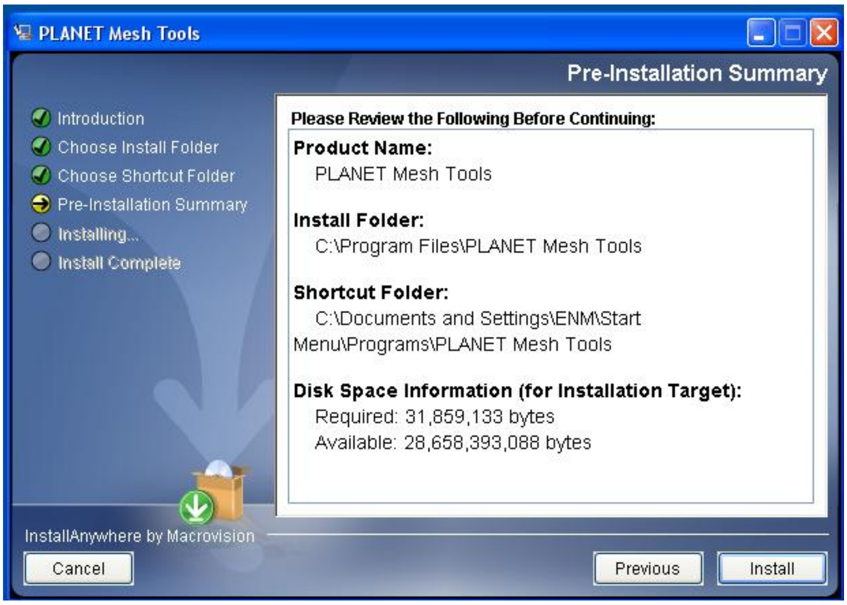
Where would you like to create product icons?

- ● In a new Program Group: PLANET Mesh Tools
- ○ In an existing Program Group: 802.11 Wireless LAN
- ○ In the Start Menu
- ○ On the Desktop
- ○ In the Quick Launch Bar
- ○ Other:
- ○ Don't create icons

□ Create Icons for All Users

Specify where the software shortcut will be created at. Press **Next** to proceed.

3.1.4 Pre-Installation Summary



Please Review the Following Before Continuing:

Product Name:
PLANET Mesh Tools

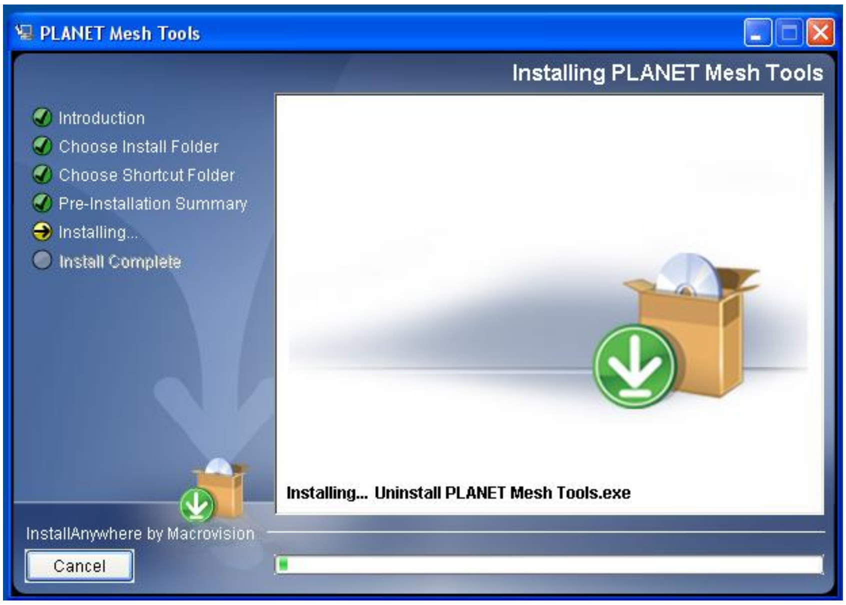
Install Folder:
C:\Program Files\PLANET Mesh Tools

Shortcut Folder:
C:\Documents and Settings\ENM\Start Menu\Programs\PLANET Mesh Tools

Disk Space Information (for Installation Target):
Required: 31,859,133 bytes
Available: 28,658,393,088 bytes

Let user have a quick review about the installation settings before start installing. Press **Install** button to start the installation.

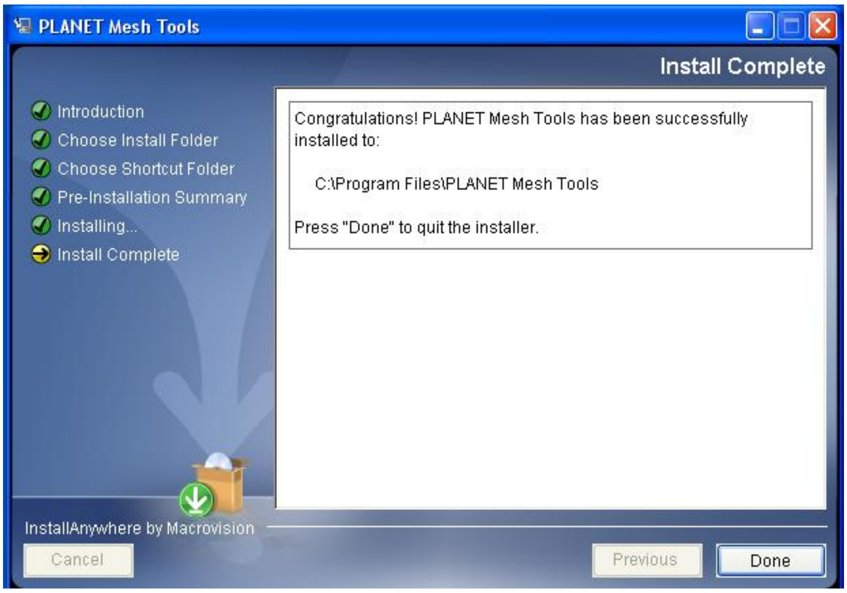
3.1.5 Installing



Installing... Uninstall PLANET Mesh Tools.exe

Installation is in progress. Once the installation is completed it will direct the user to the next step.

3.1.6 Installation Complete



Congratulations! PLANET Mesh Tools has been successfully installed to:

C:\Program Files\PLANET Mesh Tools

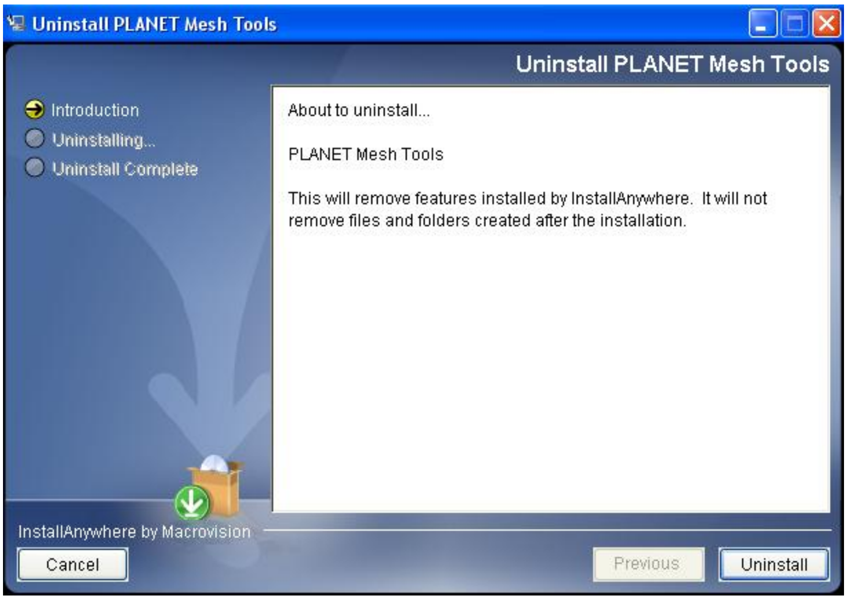
Press "Done" to quit the installer.

Indicating the installation is completed, and user can select to restart the system instantly or afterward, in order to complete the installation. Press **Done** to conclude the installation. After that, you may launch the NMS through the shortcut you created previously.

3.2 Un-installation

In order to uninstall the PLANET Mesh Network Manager from your terminal, you can get the uninstaller wizard from the software directory. The uninstaller, namely Uninstall PLANET Mesh Tools, is located at the Uninstall_PLANET Mesh Tools folder. Launch the uninstaller wizard by double-click the executable file. Follows the following steps:

3.2.1 Introduction


Uninstall PLANET Mesh Tools
Uninstall PLANET Mesh Tools
Introduction
Uninstalling...
Uninstall Complete
InstallAnywhere by Macrovision
Cancel
Previous
Uninstall

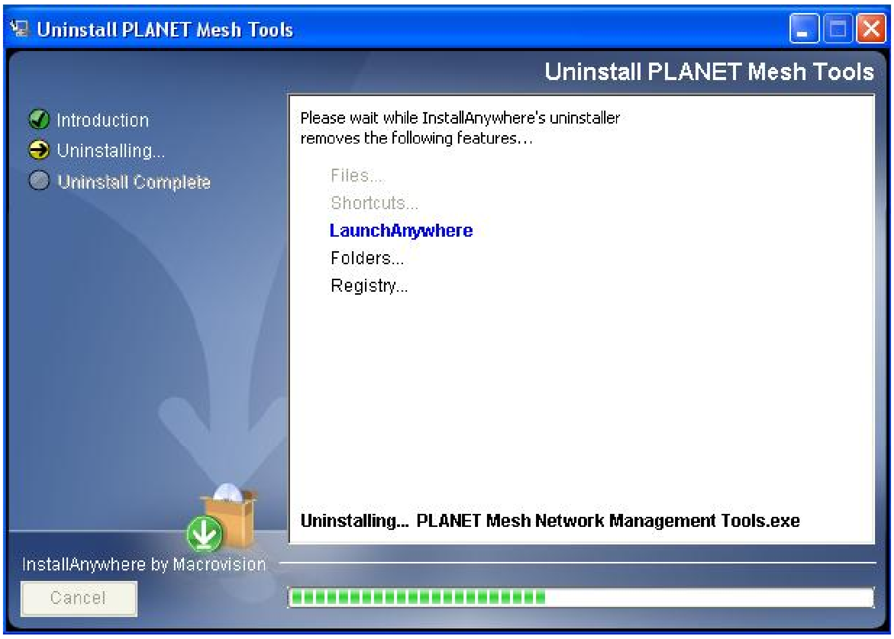
About to uninstall...

PLANET Mesh Tools

This will remove features installed by InstallAnywhere. It will not remove files and folders created after the installation.

An introduction regarding the uninstallation of the PLANET Mesh Management Tool. Click **Uninstall** to start the process.

3.2.2 Uninstalling


Uninstall PLANET Mesh Tools
Uninstall PLANET Mesh Tools
Introduction
Uninstalling...
Uninstall Complete
InstallAnywhere by Macrovision
Cancel

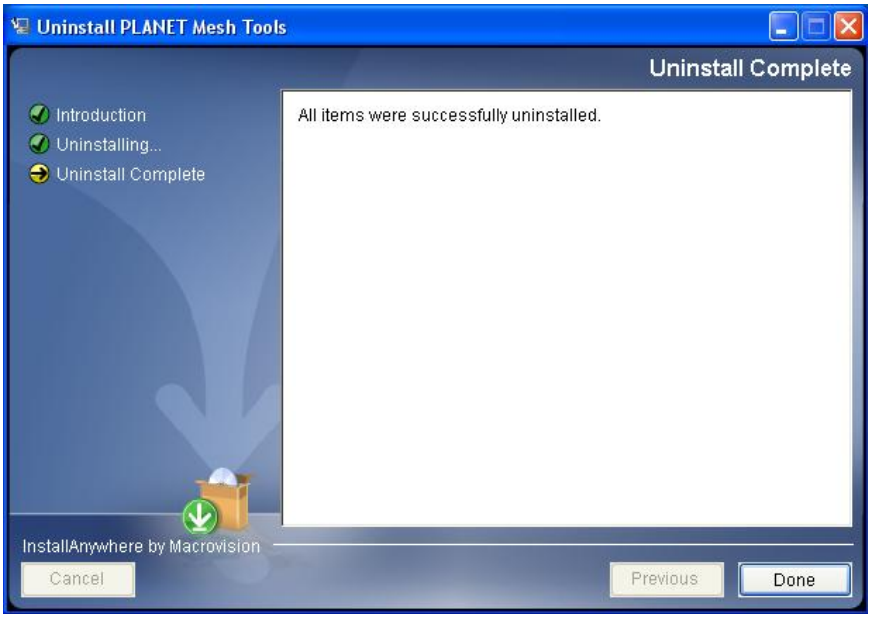
Please wait while InstallAnywhere's uninstaller removes the following features...

Files...
Shortcuts...
LaunchAnywhere
Folders...
Registry...

Uninstalling... PLANET Mesh Network Management Tools.exe

Uninstallation is in the progress. Once the progress is completed, it will automatically direct you to the next step.

3.2.3 Uninstallation Complete



All items were successfully uninstalled.

The software is uninstalled. You may choose to restart the terminal instantly or afterward in order to complete the process.

4 How to Use PLANET Mesh Network Management Tools

4.1 Quick Start

First of all, make sure the terminal where you installed your PLANET Mesh Network Management Tools is connected to the network, via Wireless or Wired LAN. Then, launch the NMS at the location where you install it.

For a Layer 3 Mesh network:
Click the **Create Map** button on the toolbar to generate a new map profile. A dialog box would appear, select **SNMP Map** and enter the name of the new profile. After that, hit the **OK** button to complete the set up. A new map will be inserted into the NMS.

Then, click on the drop-down list on the toolbar of the new profile, where it prompts users to insert the Scan IP Address, the destination IP Address to be scanned. Enter the desired IP and click the button next to the list to save the IP. Finally, select the **Start Scan** button on the map’s toolbar, the scan will be initiated and run. The result of the scan will be plotted on the map area. User is free to adjust the position of the found-unit on the map.

For a Layer 2 Mesh network:
Prior to set up the utility, user is required to add the IP address of the NMS terminal on the web page (Management > NMS Addresses) of Layer 2 nodes.

After the Layer 2 node configuration is done, activate the NMS and click the **Create Map** button. A dialog box would appear, select **Layer-2 Map** and enter the name of the new profile. After that, hit the **OK** button to complete the setup. A new map will be inserted into the NMS.

Before shutting down the NMS, user can save the profile settings, including the coordinate of the found Mesh AP units on the map, by click on the **Save Map** button on the map toolbar. The saved profile can be loaded directly to the NMS next time using the **Open Map** button on the toolbar.

For further description regarding the functions and features of the PLANET Mesh Network Management Tools, user may refer to the following section.

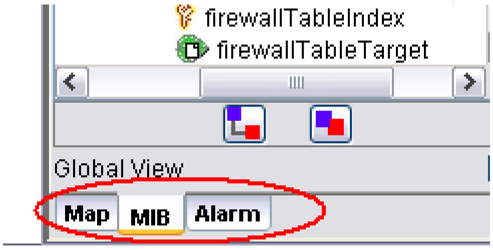
4.2 Software Overview & Features

4.2.1 Software Layout

Before we proceed further, let us have an overview at the layout of the NMS. Basically, the PLANET Mesh Network Management Tools is consists of three major sections:

- Map Container
- MIB Reader
- Alarm Viewer

User can switch the view of the NMS by select the tabs at the left bottom corner, as illustrated, or through the menu bar.



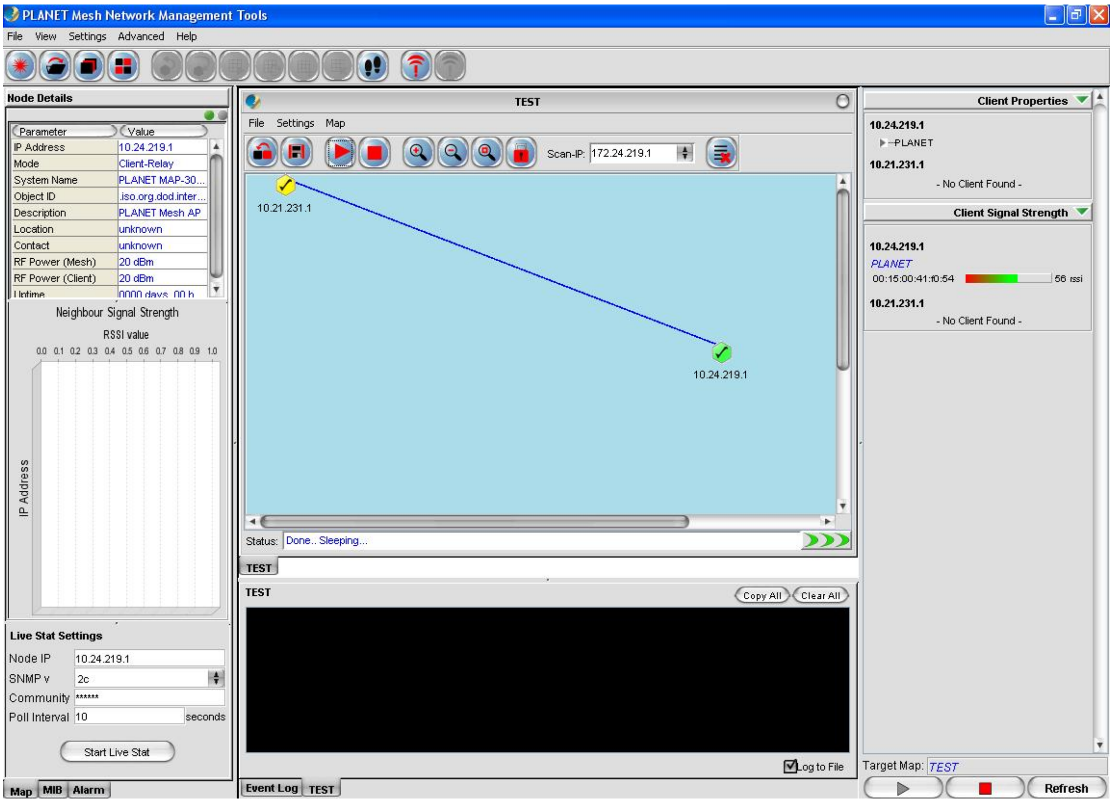
4.2.1.1 Map Container

The Map Container is the section where user can monitor and manage the mesh network. The network will be displayed in the form of graphical topology map, and the status will be updated periodically.

The center frame of the Map Container is the space to plot the topology map. More than one map can be created and run simultaneously. The status of the map will be logged to the status pane at the bottom of the map. Each topology map has its own status pane.

The panel at the left of the map space is the Node Details panel. It is used to display the properties of the selected Mesh AP unit on the topology map. The information of the AP will be loaded into the table, and the graph below the table shows the signal strength between the selected AP with its neighbour APs. The column at the bottom of this panel is used to invoke the live stat monitoring feature.

The right panel, meanwhile, is to display the details of the clients associated to the Mesh AP unit. The panel is divided into two parts, the Client Properties and Client Signal Strength portion. Each portion will be automatically updated every minute, to provide the admin user the live result regarding the clients.



Parameter	Value
IP Address	10.24.219.1
Mode	Client-Relay
System Name	PLANET MAP-30...
Object ID	.iso.org.dod.inter...
Description	PLANET Mesh AP
Location	unknown
Contact	unknown
RF Power (Mesh)	20 dBm
RF Power (Client)	20 dBm
Uptime	0000 days 00 h

Node IP 10.24.219.1

SNMP v 2c

Community ******

Poll Interval 10 seconds

Scan-IP: 172.24.219.1

Status: Done.. Sleeping...

Client Properties

10.24.219.1
- PLANET

10.21.231.1
- No Client Found -

Client Signal Strength

10.24.219.1
PLANET
00:15:00:41:f0:54 56 rssi

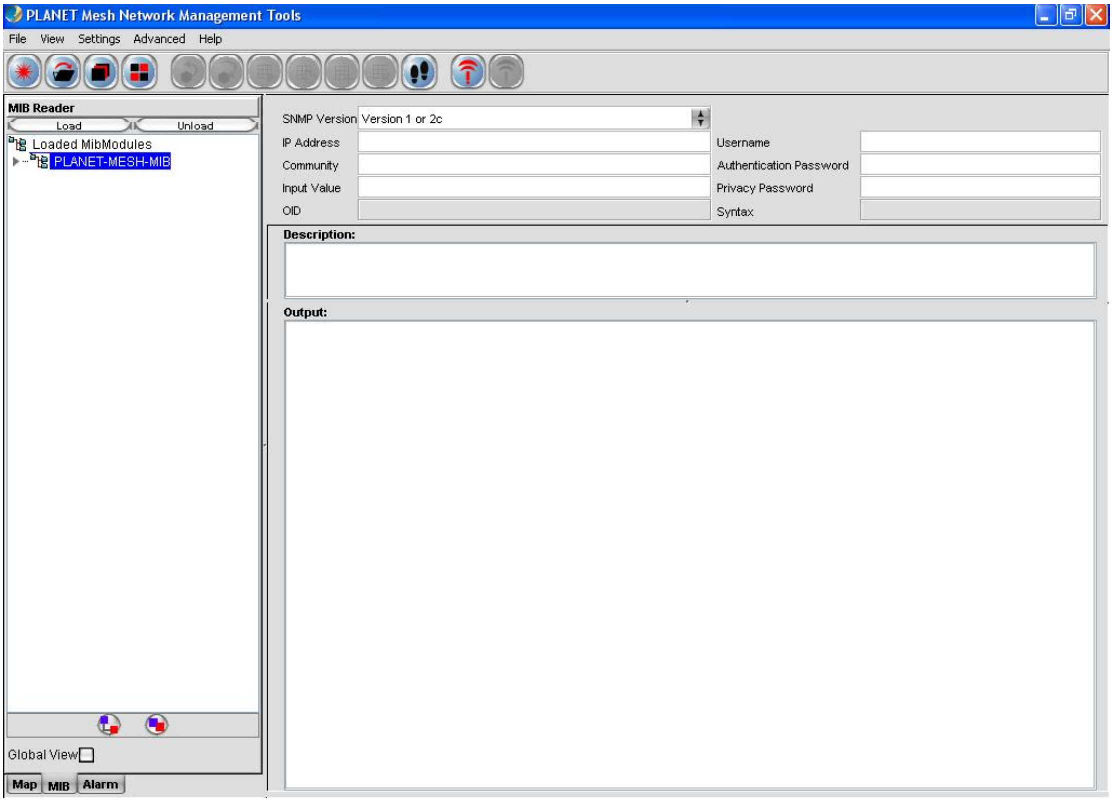
10.21.231.1
- No Client Found -

Target Map: TEST

☑ Log to File

4.2.1.2 MIB Reader

The MIB Reader provides user a simple user-interface to retrieve as well as configure the settings of the Mesh AP unit through the standard or vendor proprietary MIB files. With the correct community and password, user can perform the SNMP actions such as SNMPGet, SNMPSet and SNMPTable.



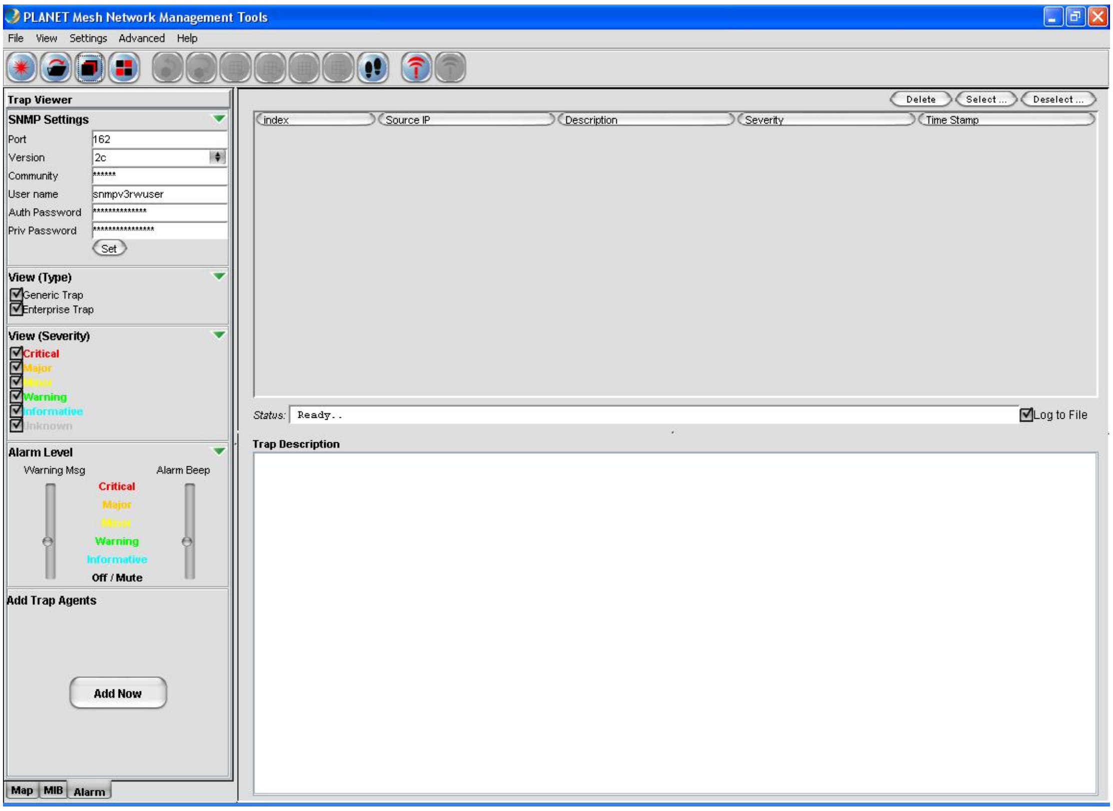
SNMP Version: Version 1 or 2c

The left pane displays the list of MIB and its tree. User can load and unload MIB file from the desired location. More than one file can be loaded into the MIB Reader. In order to read or set an item, expand the MIB tree, select the desired node. Select the SNMP version; fill in the IP Address and other necessary keyword. Then click on the command button (**SnmpGet, SnmpSet, SnmpWalk, Load Table,** etc..) on the toolbar. The output will be shown on the Output column.

4.2.1.3 Alarm Viewer

The Alarm Viewer is a trap receiver. It received the SNMP alarms and notifications directed by the Mesh AP units and display in the table at the center frame. Select the table entry in order to view the description of the trap.

Note that the table is a read-only table, which displays the trap's source IP Address, description, severity and the time when the trap or alarm was caught. These alarms should be deleted once they were reviewed and resolved, by clicking the **Delete** button.



PLANET Mesh Network Management Tools
File View Settings Advanced Help
Trap Viewer
Delete Select ... Deselect ...
index Source IP Description Severity Time Stamp

SNMP Settings

Port 162

Version 2c

Community ******

User name snmpv3rwuser

Auth Password **************

Priv Password ****************

View (Type)

☑ Generic Trap

☑ Enterprise Trap

View (Severity)

☑ Critical

☑ Major

☑ Minor

☑ Warning

☑ Informative

☑ Unknown

Alarm Level
Warning Msg
Alarm Beep
Critical
Major
Minor
Warning
Informative
Off / Mute
Add Trap Agents
Add Now
Map MIB Alarm

Status: Ready..

☑ Log to File

Trap Description

4.2.2 Toolbar Reference

This section provides a quick reference for the buttons in the toolbar of the NMS. The description of the toolbar of the NMS is illustrated at the table below:

Button	Name	Function
	Create Map	Create a new topology map profile
	Open Map	Open a pre-saved topology map profile
	View Tile	View the topology map in grid layout
	View Cascade	View the topology map in cascade layout
	SnmpGet	SnmpGet the data from MIB tree
	SnmpSet	SnmpSet the data from MIB tree
	Load Table	Load the SNMP table from MIB tree
	Refresh Table	Refresh the SNMP table from MIB tree

	Add Table Row	Add a row to SNMP Table
	Del Table Row	Delete a row from SNMP Table
	SnmpWalk	Walk the selected item from the MIB tree
	Start Trap	Initiate the Alarm Host system
	Stop Trap	Stop the Alarm Host system

On the other hand, the following table shows the description of the toolbar of the map container:

Button	Name	Function
	Import Background	Import an image file to use as the background image of the topology map
	Save Profile	Save the current topology map
	Scan Start	Start the network scanning (SNMP Map only)
	Scan Stop	Stop the network scanning (SNMP Map only)
	Initiate Port	Open port to listen to Layer-2 notification (Layer-2 Map only)
	Close Port	Close Layer-2 notification port (Layer-2 Map only)
	Zoom In	Zoom in the topology map by 25%
	Zoom Out	Zoom out the topology map by 25%
	Zoom Fit	Zoom the topology map to a size that fit the screen
	Lock	Lock the AP units on the map
	Unlock	Unlock the AP units on the map
	Block List	Open the block list window

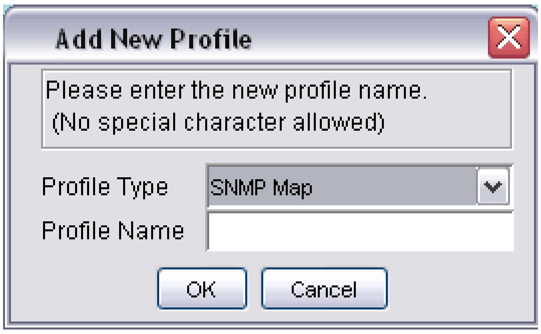
4.2.3 Features

4.2.3.1 Create Map

In the NMS, two topology maps are available: SNMP Map and Layer-2 Map. These two types of map look similar. The main difference between them is the method to get the topology information.

- The **SNMP Map** is the ordinary type, where it uses the SNMP protocol to collect the topology from the nodes discovered, and then plot the map using the collaborate data.
- Whereas the **Layer-2 Map** opens a specific port to listen for the notification from the nodes, in order to plot the map. Prior to this, user is required to add the information of the NMS terminal (IP Address) to the node. Thus in fact, the Layer-2 Map can receive the notification not only from the layer-2 mode AP, but any other mode as well, as long as the NMS Address table is set.

In order to create a new Topology map profile, user can click on the **Create New** button on the main toolbar, or select File > Create New from the menu bar. A window would turn out to prompt user for the type and name of the new map. User may select the type of the profile from the drop down list, and enter the name in the provided column.



Please enter the new profile name.
(No special character allowed)

Profile Type: SNMP Map
Profile Name:

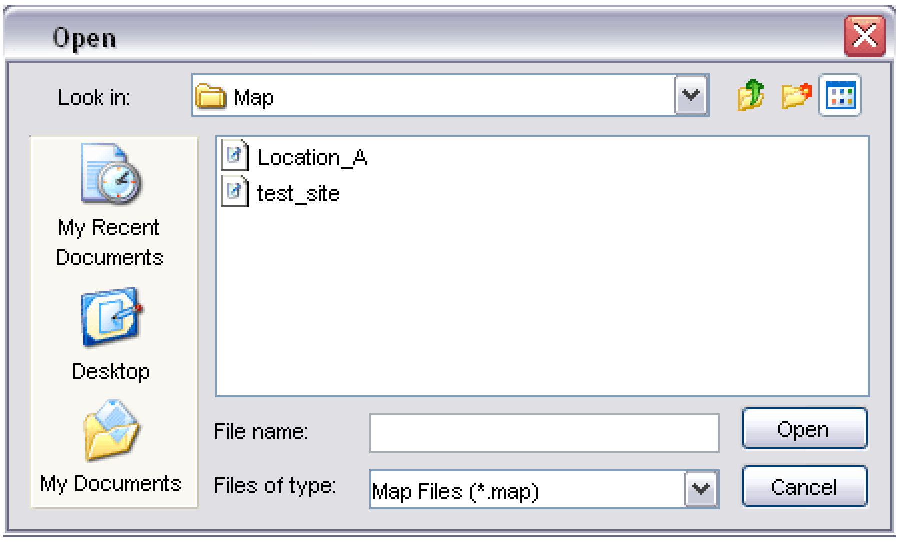
Please be aware that special character such as #, $, % (except _), are not allowed to use as the name of the topology map name to avoid data corruption, since the name of the map will be used as the header of their data file. On the other hand, the system also not allow user to create a new profile with the name of the existing map in the NMS.
Two Profile Types can be found, **SNMP Map** and **Layer 2 Map**. Please chose **SNMP Map** for Layer 3 mode Mesh Network Management and **Layer 2 Map** for Layer 2 Mode Mesh Network Management.

Hit the **OK** button to proceed, or **Cancel** to close the window.

⚠ **Note** Please make sure your Layer 2 Mesh Nodes are pre-configured for this MnM installed PC. Otherwise, MnM can not display your Mesh nodes in the map also cannot show the correct information at the mean time. Please also refer to Web guide section 3.5.10 for more.

4.2.3.2 Open Map

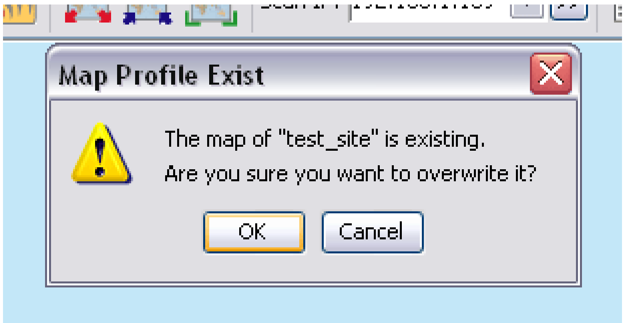
In stead of create a brand new topology map, user can re-open the map profile that has been saved previously. Click the **Open Map** button, or select **File > Open** Map from menu bar, a file chooser window would appear on the screen, to prompt user to choose a map. Select the desired one, and hit the **Open** button. The profile will be loaded to the NMS with all its settings.



4.2.3.3 Save Map

As mentioned previously, the settings of the map profile can be saved to be loaded in the future. Details of the map, for instance, the coordinate and SNMP passwords of the Mesh AP units on the map, background image and block list, will be saved as a setting file.

In order to save a profile, select the **Save Map** button or **File > Save Map** from the map container toolbar of that particular map profile you wish to save. Note that if user is trying to save a map profile that has a same name as one of the existing profile, a warning message would appear to get confirmation from the user to overwrite the file. To proceed with the action, click the **OK** button.



The map of "test_site" is existing.
Are you sure you want to overwrite it?

By default, the profile will be saved to the Map folder in the program's directory, with the name of the map profile and extension .map or .l2map.

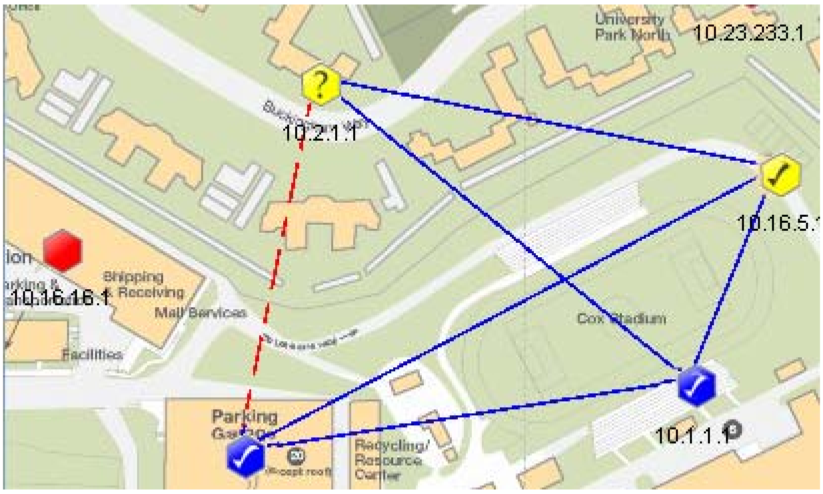
4.2.3.4 Topology Map

The topology map is actually the graphical representation of the actual Mesh network topology which is being scanned. When a new scan is initiated, the result of the scan will be processed by the NMS, and output to the map.

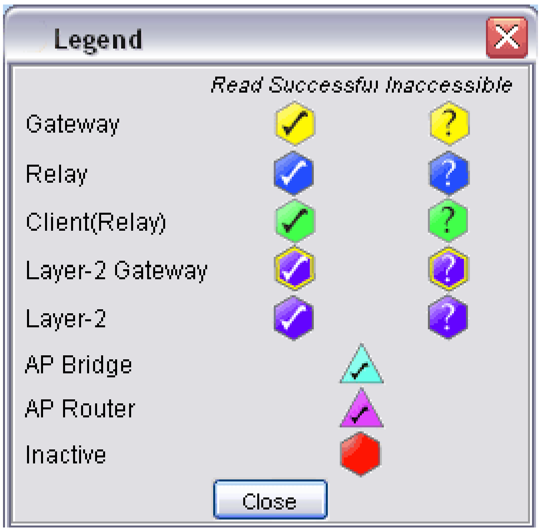
The AP unit would appear in different colors:-

Icon	Indication
🔴	Inactive AP
🟡✓	Accessible gateway AP
🟡?	Inaccessible gateway AP
🔵✓	Accessible relay AP
🔵?	Inaccessible relay AP
🟢✓	Accessible client-relay AP
🟢?	Inaccessible client-relay AP
🟡🟣✓	Layer-2 gateway AP, which notified the NMS
🟡🟣?	Layer-2 gateway AP, which did not notify the NMS (discovered as neighbour)
🟣✓	Layer-2 AP, which notified the NMS
🟣?	Layer-2 AP, which did not notify the NMS (discovered as neighbour)
△✓	AP Bridge

▲ AP Router



The blue line in between the APs designates the solid link; whereas the red, dashed line shows the indirect link. On the other hand, user may hit the **Help > Legend** option from the menu bar to view the legend regarding the topology.



Legend

	Read Successful	Inaccessible
Gateway	✓	?
Relay	✓	?
Client(Relay)	✓	?
Layer-2 Gateway	✓	?
Layer-2	✓	?
AP Bridge	▲	
AP Router	▲	
Inactive	●	

4.2.3.5 Set up New Scan

In order to set up a new scan for a SNMP topology map, click on the **Start Scan** button, or select **Map > Start Scan** from the menu bar. Conversely, hit the **Stop Scan** button or select **Map > Stop Scan** to halt the scanning process. The status of the map will be updated periodically, hence whenever there is a change in the network, user might be able to monitor via the NMS. The status bar at the bottom of the map displays the status of the scan.

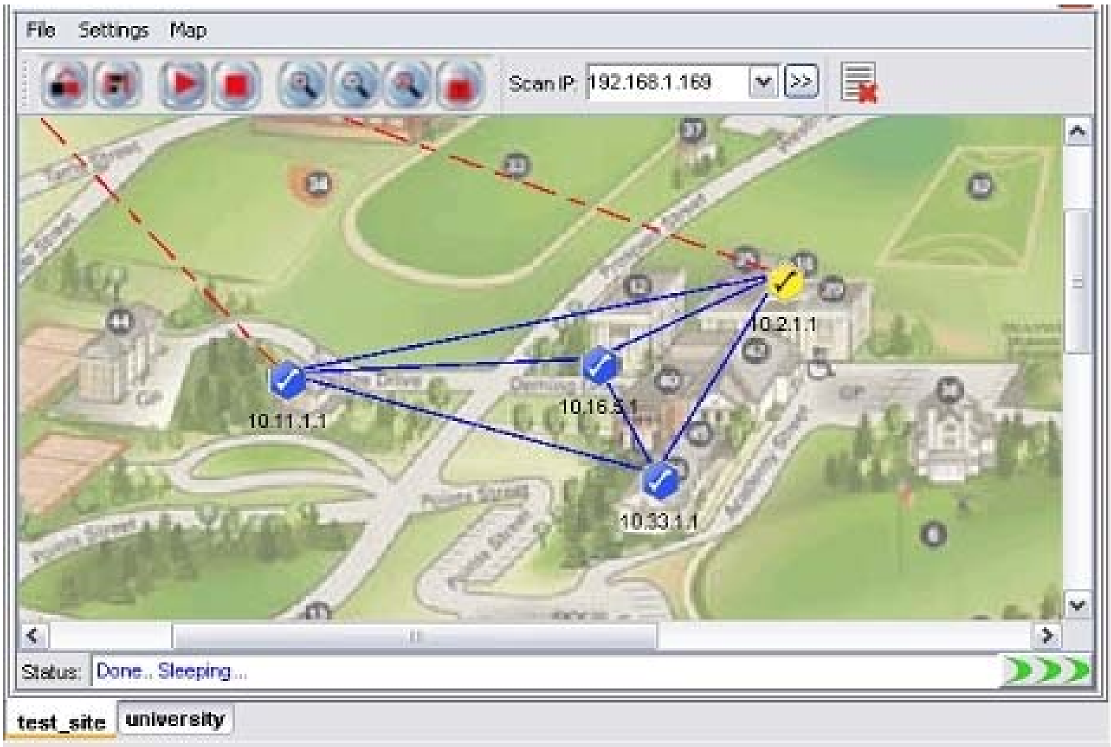
On the other hand, in order to set up a new scan for the Layer-2 topology map, click on the **Initiate Port** button, or select **Map > Initiate Port** from the menu bar. The map will receive the notification sent by the AP and plot the topology on the map. Conversely, hit the **Close Port** button or select **Map > Close Port** from the menu bar to stop listen to the notification.

Every new found Mesh AP unit will be place on the right top angle on the map, with zero coordinate. Then user is free to move the AP unit around the map. Once user completes the positioning, save the map, and the system will remember the new coordinates in the future scan.

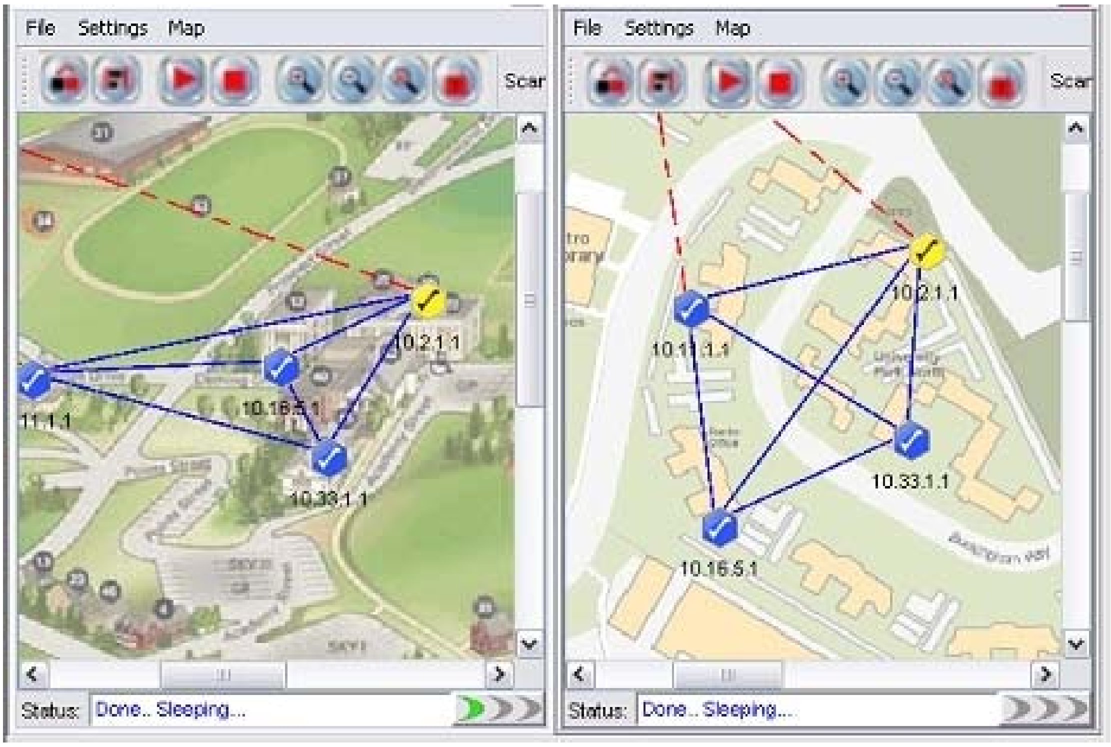
4.2.3.6 Map View

More than one topology map can be loaded to the NMS at the same time. By default, the maps are viewed in cascade mode, where user needs to click on the tab at the bottom to switch the map to view.

In order to change the view type, click the **Tile** button on the main toolbar, or select View > Tile from the menu bar. The tile mode arranges the topology maps in a grid layout. To convert the view mode to cascade, hit the **Cascade** button, or View > Cascade. The following figures illustrate the difference between the two modes.



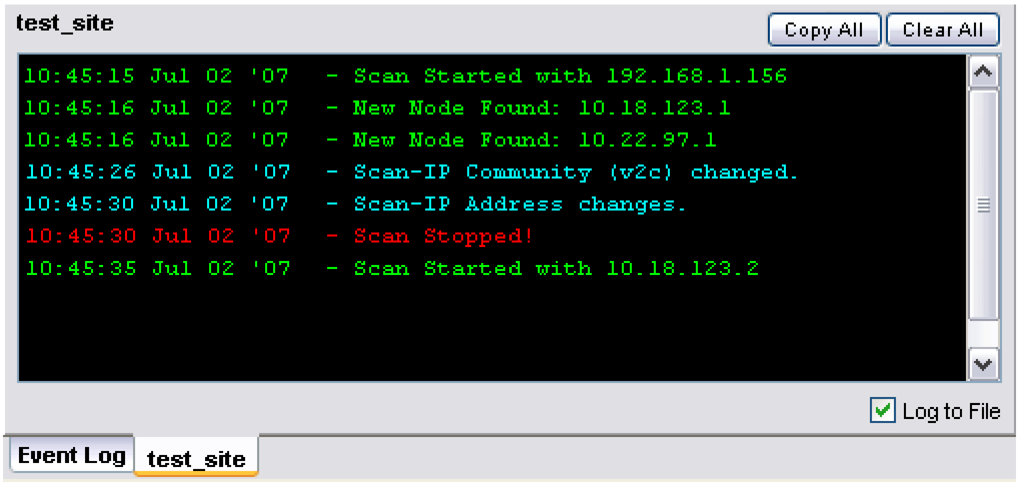
(Cascade mode)



(Tile Mode)

4.2.3.7 Status Pane

The status pane is located at the bottom of the map container. It displays the nodes' status with the time and date; enable users to keep track of the changes in the topology.



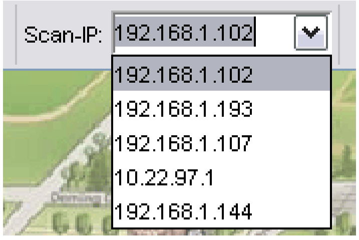
```
10:45:15 Jul 02 '07  - Scan Started with 192.168.1.156
10:45:16 Jul 02 '07  - New Node Found: 10.18.123.1
10:45:16 Jul 02 '07  - New Node Found: 10.22.97.1
10:45:26 Jul 02 '07  - Scan-IP Community (v2c) changed.
10:45:30 Jul 02 '07  - Scan-IP Address changes.
10:45:30 Jul 02 '07  - Scan Stopped!
10:45:35 Jul 02 '07  - Scan Started with 10.18.123.2
```

The type of message can be varied by the color of the text. Green text indicating positive message such as scan started or nodes found; red text shows the negative message such as nodes down or timeout; whereas cyan text displaying system message, for instance, system settings changed.

The **Copy All** and **Clear All** buttons on the top of the pane performs the copy and delete text action in the status pane. Tick the checkbox at the bottom to log the status message to the alarm log file, which will be saved to the folder Alarm_Log at the install directory.

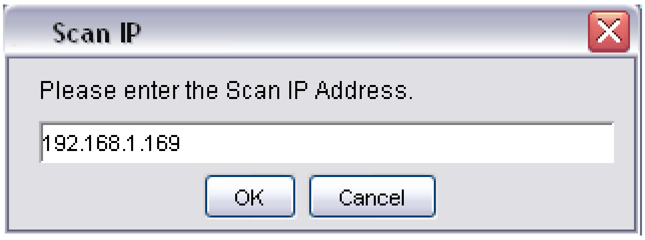
4.2.3.8 Scan IP Address

The Scan IP Address is the IP Address that the scanning process uses when initiate a scan for a SNMP Map.



User might enter the IP Address at the drop down list, or choose from the list. In order to apply the new Scan IP, user is required to restart the network scanning. (A running scan will be stopped when a new IP Address is selected.)

On the other hand, the Scan IP can also be set by selecting **Settings > Scan IP** from the map container’s toolbar. A window would appear to prompt user for the new IP Address. Hit the **OK** button to apply the change.



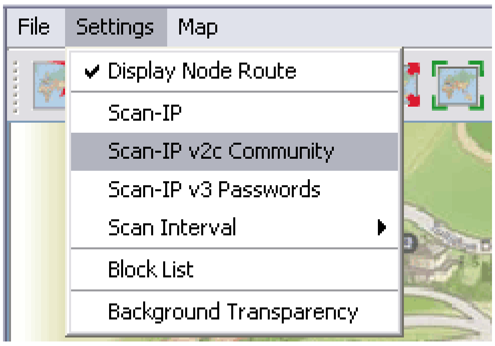
Please enter the Scan IP Address.

192.168.1.169

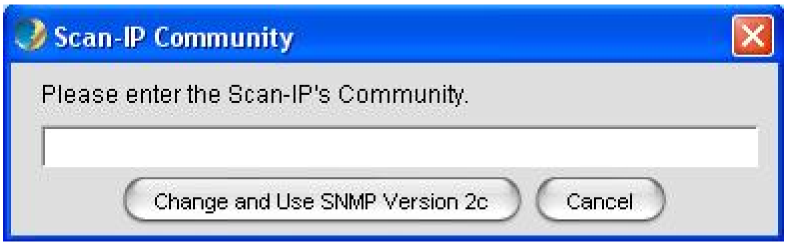
4.2.3.9 SNMP Community / Passwords (for Scan-IP)

The PLANET Mesh Network Management Tools use the SNMP method to read the topology of the network. There are two types of SNMP key used for the topology scan, which are the Scan-IP key and the AP Unit key. More details about the latter please click here.

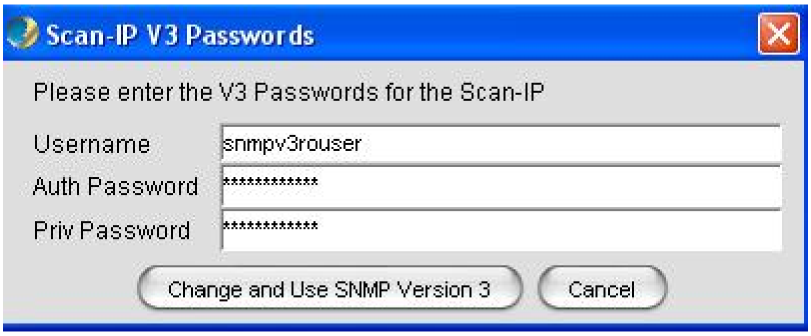
Commonly, the use of SNMP varies by its version. If a user select version 2c, the SNMP key to use is a community; on the other hand, if version 3 is used, the SNMP key will be a SNMPv3 username, with its corresponding authentication password and privacy pass phrase. As you can see throughout this document, every feature that implements SNMP will have both options (use version 2c or 3).



Basically, the Scan-IP key is the SNMP key that used for the Scan-IP which initiates the scan. In order to configure the community of the Scan-IP, select **Settings > Scan-IP v2c Community** from the map container menu. On the other hand, select **Settings > Scan-IP v3 Passwords** to change the SNMP version 3 Passwords. A window would turn up to prompt user for the new key(s).


Scan-IP Community

Please enter the Scan-IP's Community.


Scan-IP V3 Passwords

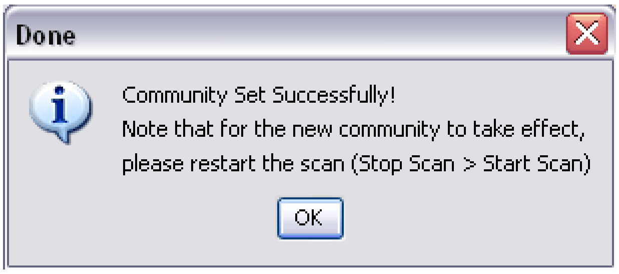
Please enter the V3 Passwords for the Scan-IP

Username snmpv3rouser

Auth Password *************

Priv Password *************

Press **Change and Use SNMP Version X** button to proceed. If the change is successfully, the following dialog box would appear, to remind user to reset the scan in order to let the new community or passwords to take effect.


Done

Community Set Successfully!
Note that for the new community to take effect,
please restart the scan (Stop Scan > Start Scan)

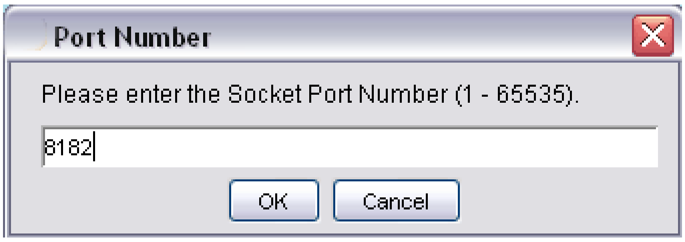
The default value for Scan-IP:

Community: public
Username: snmpv3rouser
Password: snmpv3password
Passphrase: snmpv3passphrase

4.2.3.10 Socket Port

The notification of an AP node is sent according to its NMS Address Table. The table defines the IP Address and port number of the destination (NMS). For instance, if the admin has added a table entry with port number 8000 at the AP, the NMS user can change the socket port number to 8000 in order to receive the notification.

In order to update the socket port, select **Settings > Socket Port** from the menu bar. A dialog box would appear on the screen to prompt for the port number, which range from 1 to 65535. Hit **OK** to confirm the change.



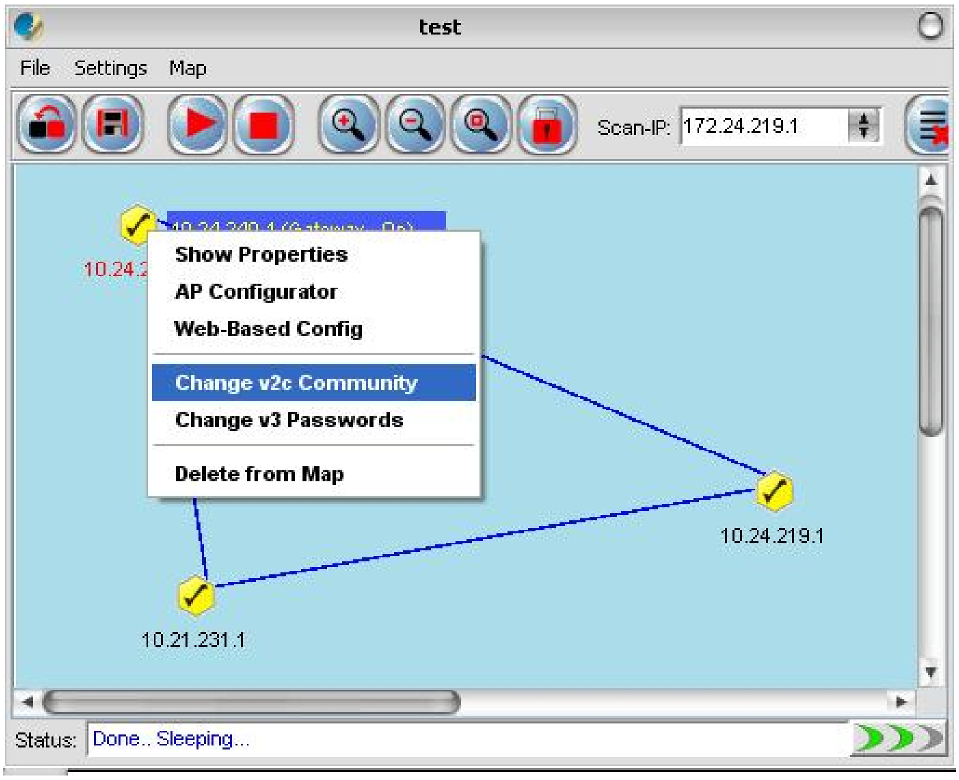
Port Number

Please enter the Socket Port Number (1 - 65535).

8182

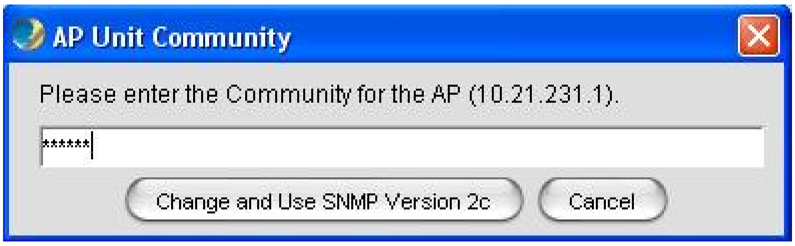
4.2.3.11 SNMP Community / Passwords (for AP Unit)

In case if a Mesh AP utilizes a different community or passwords from the others, the NMS might fail to read the topology from it. Hence, user might need to edit the individual AP unit SNMP keys, by right-click the desired active node. Select **Change v2c Community** from the popup menu to change the community; or click **Change v3 Passwords** to change the v3 keys; enter the correct value in the dialog box and click **Change and Use SNMP Version X**.



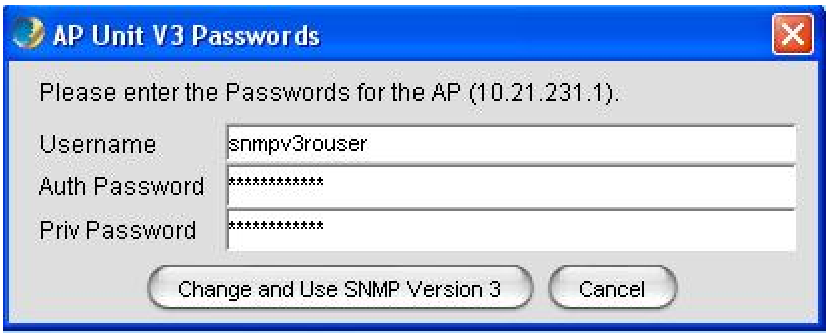
Scan-IP: 172.24.219.1

Status: Done.. Sleeping...



Please enter the Community for the AP (10.21.231.1).

******



Please enter the Passwords for the AP (10.21.231.1).

Username: snmpv3rouser

Auth Password: ************

Priv Password: ************

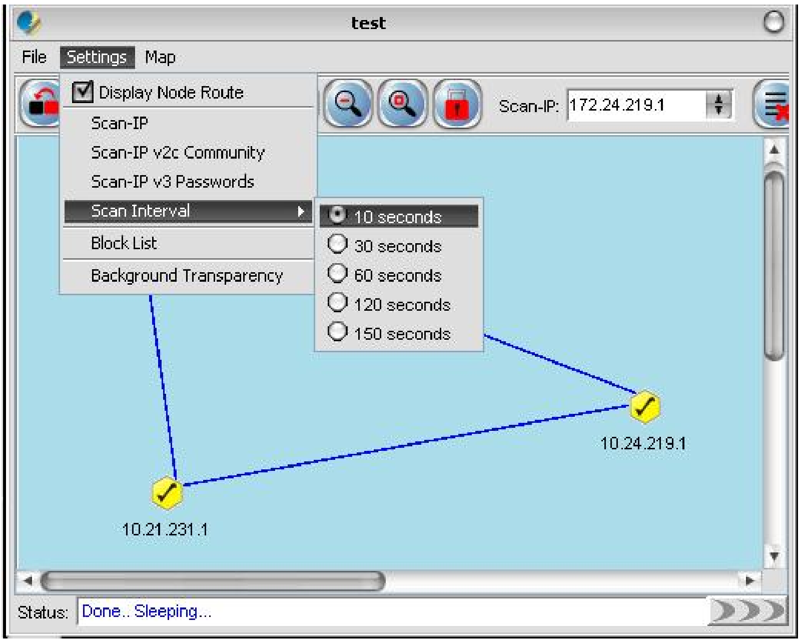
Note that the AP Unit Keys is also used for read the Node Details and Client Properties. The default SNMP version and keys of the Mesh AP is inherited from the Scan-IP that found them.

4.2.3.12 Scan Interval

The scan interval defines the time interval between every round of scanning. By default, the NMS will sleep for 10 seconds once a network scan is completed. User may change the time interval by select **Settings > Scan Interval**, and choose the desired time interval. The available options:

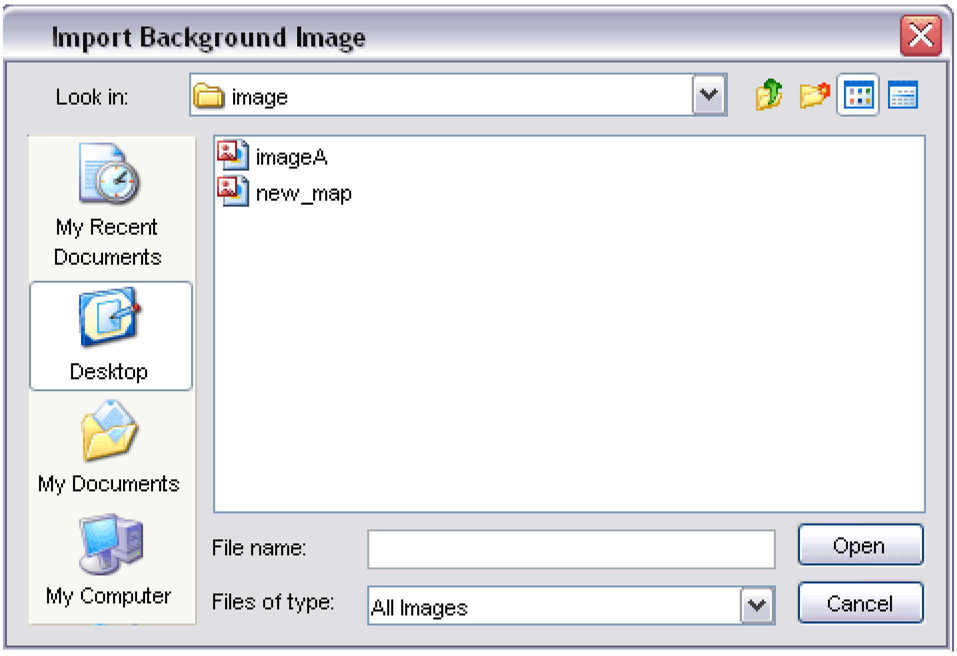
- 10 seconds
- 30 seconds
- 60 seconds
- 120 seconds
- 150 seconds

The changes will take effect immediately.



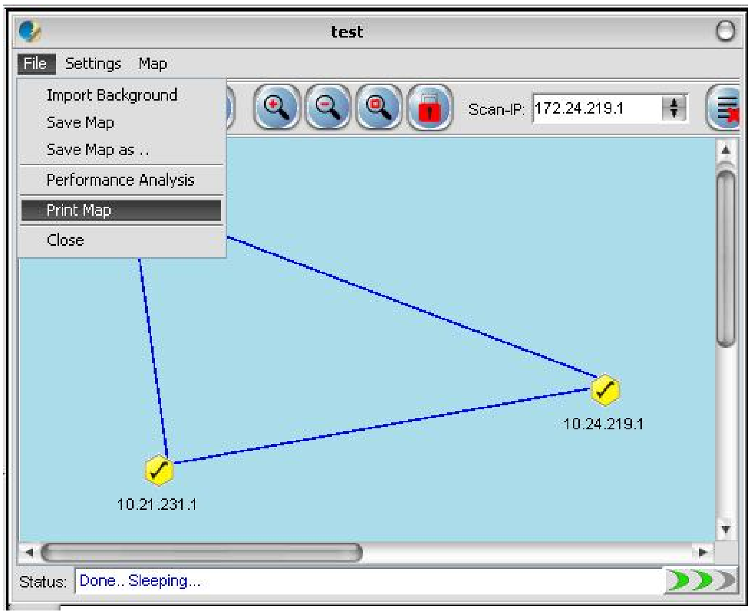
4.2.3.13 Import Background Image

User can change the background of the topology map by import any desired image file from other resource. Click on the **Import Background Image** button, or select **File > Import Background** from the map container's menu bar. A file chooser window would appear, to prompt user for the image file that wished to import.



After select a image file (.jpg, .gif, .png ..etc), click the **Open** button. The new image will be loaded into the topology map.

4.2.3.14 Map Print

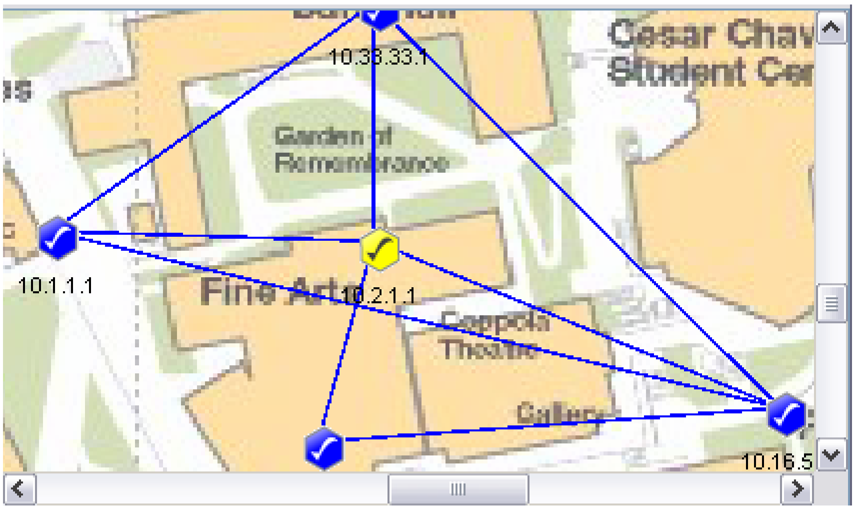


The NMS also provide the printing feature, where user is able to print the whole map by just select the **File > Print Map** option from the Map Container menu bar. Then it will redirect the map to the printer connected to the terminal where you run the NMS.

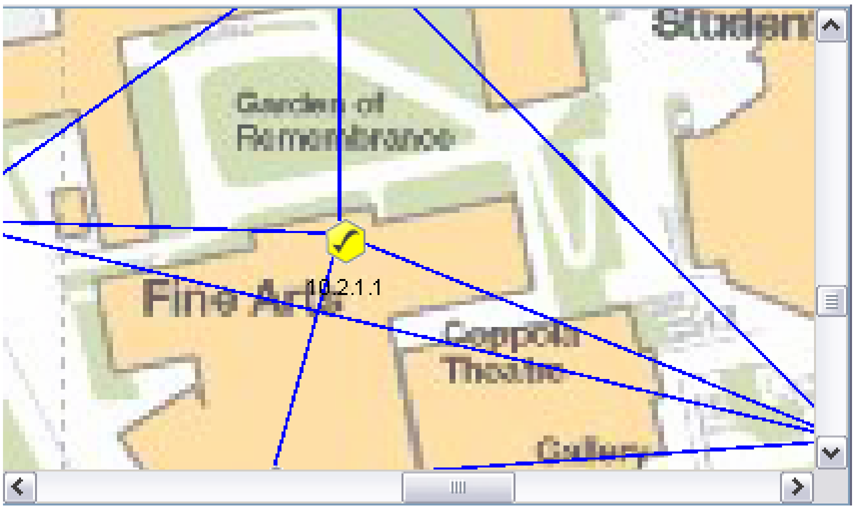
4.2.3.15 Map Zoom

As a graphical solution for a network system, the PLANET Mesh Network Management Tools provides the zooming feature for the user to manage the topology map more efficiency. Three options are available: Zoom In, Zoom out and Zoom Fit.

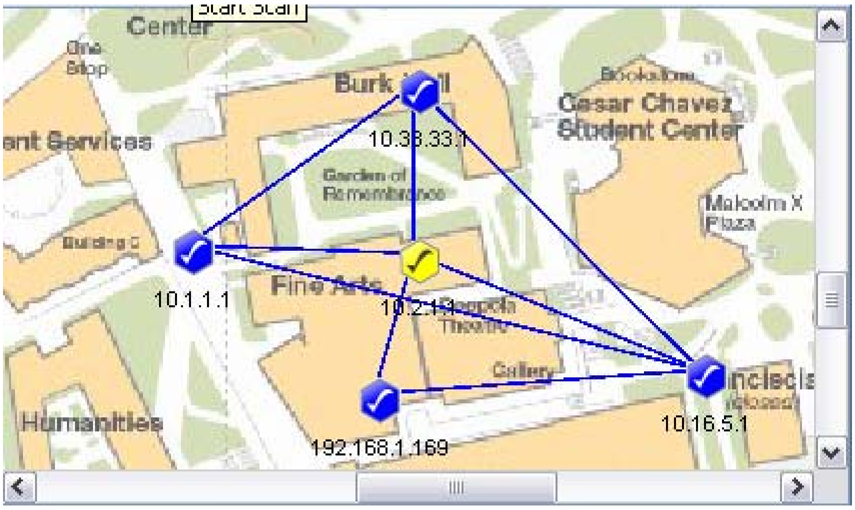
The Zoom In and Zoom Out feature enable user to enlarge and minimize, respectively, at the scale of 25%. Whereas the Zoom Fit feature will resize the topology map to the most suitable size to fit in the screen. The following figures illustrate the effect of the zoom features.



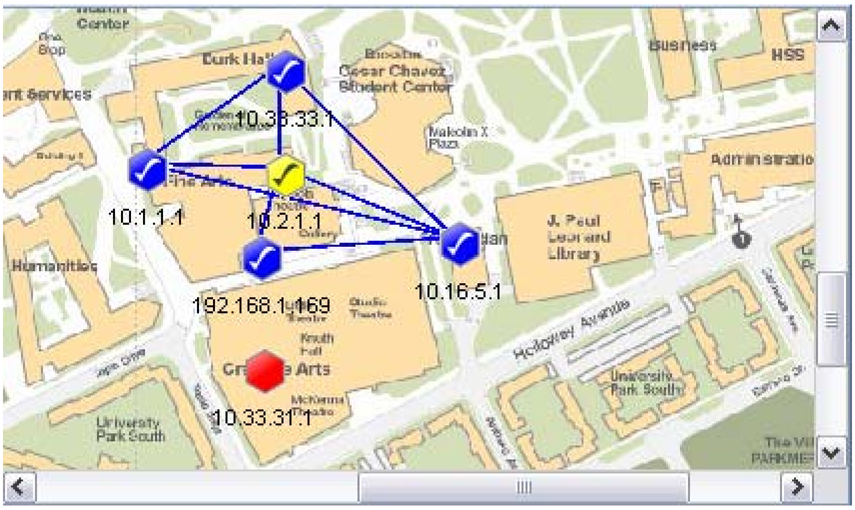
(Original size)



(Zoom In)



(Zoom Out)

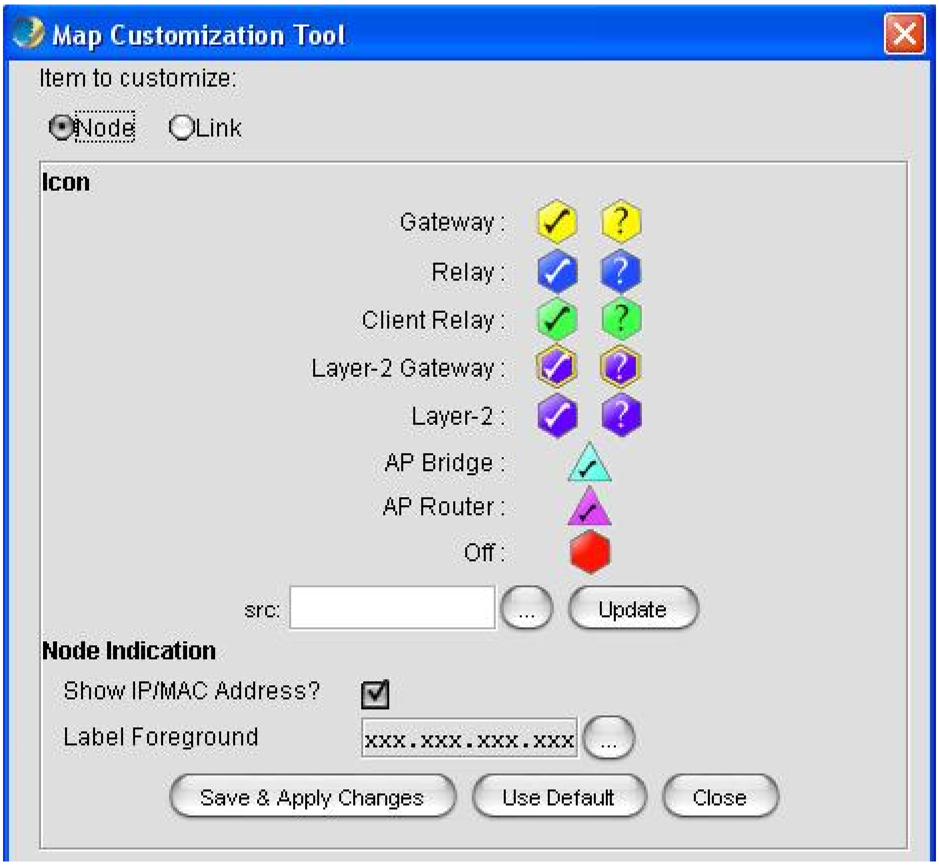


(Zoom Fit)

4.2.3.16 Customize Map

This feature provides user the flexibility to change the look and feel of the topology map, by replacing the existing AP unit image and the link between APs. User can import their custom-made icon, or adjust the color to fit their visual requirement.

The method is straight forward. Select **Settings > Customized Map** from the NMS menu bar, to invoke the Map Customization Tool window, as illustrated.



Map Customization Tool

Item to customize:

● Node ○ Link

Icon

Gateway :

Relay :

Client Relay :

Layer-2 Gateway :

Layer-2 :

AP Bridge :

AP Router :

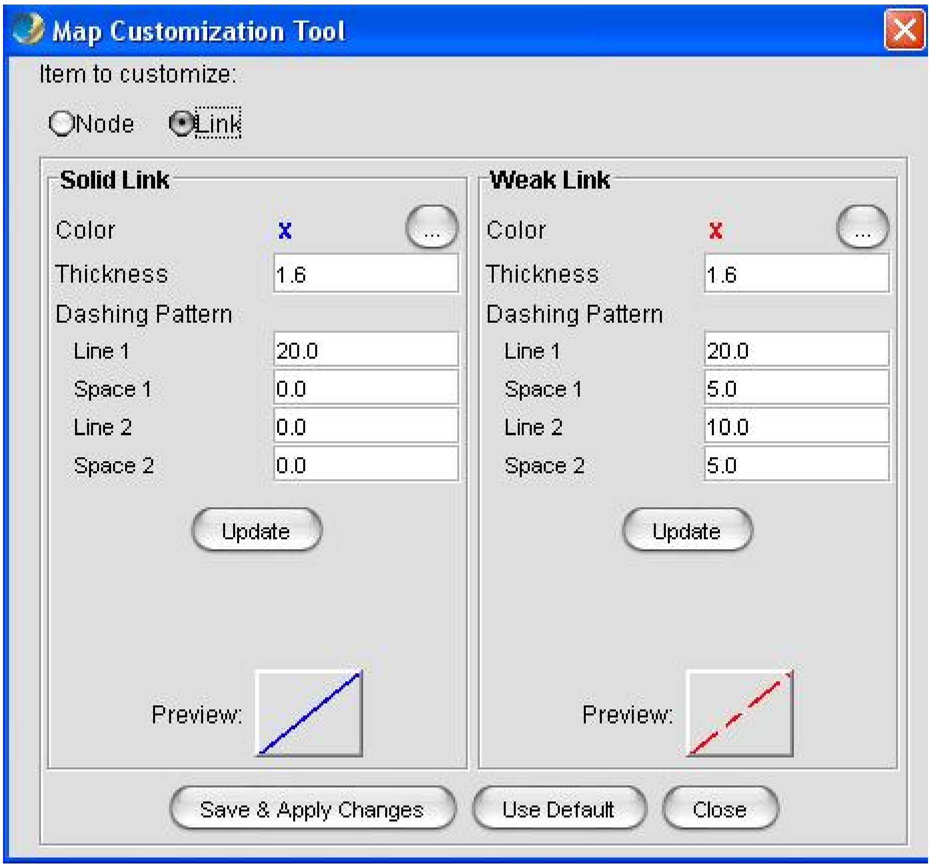
Off :

src:

Node Indication

Show IP/MAC Address? ☑

Label Foreground xxx.xxx.xxx.xxx



Map Customization Tool

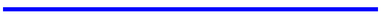
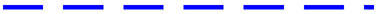
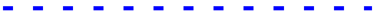
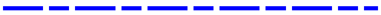
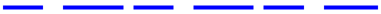
Item to customize:

○ Node ● Link

Solid Link		**Weak Link**	
Color	x	Color	x
Thickness	1.6	Thickness	1.6
Dashing Pattern		Dashing Pattern	
Line 1	20.0	Line 1	20.0
Space 1	0.0	Space 1	5.0
Line 2	0.0	Line 2	10.0
Space 2	0.0	Space 2	5.0

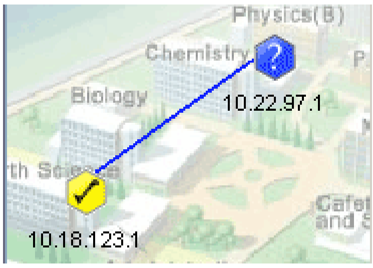
As you can see from the figures, the customization can be divided to two parts, the Node and the Link. At the Node part, user may select the icon that need to be updated, and then fill in the path of the new image (or click the "…" button to choose from the file chooser window). Hit the **Update** button to update the new image icon. Besides, user can also decide whether to show the indication of the AP-unit, which is the IP Address, by using the available checkbox; and alter the foreground color of the IP Address using the "**…**" button to select a desired color from the popup window. Hit the **Save & Apply Changes** button to commit the changes. The **Use Default** button enables the user to restore the default settings of the AP unit look and feel.

Meanwhile, in order to change the style of the link, switch the Map Customization Tool to the Link page. User can change the color by hitting the "**…**" button to select a desired color from the popup window. Then key in the thickness of the link and its dashing pattern. The dashing pattern defines the way the dashed link look like. The following table explains how to use the dashing pattern. After fill in the data, user may click the **Update** button to update the image at the preview. Once confirm the changes, select the **Save & Apply Changes** button to commit the change.

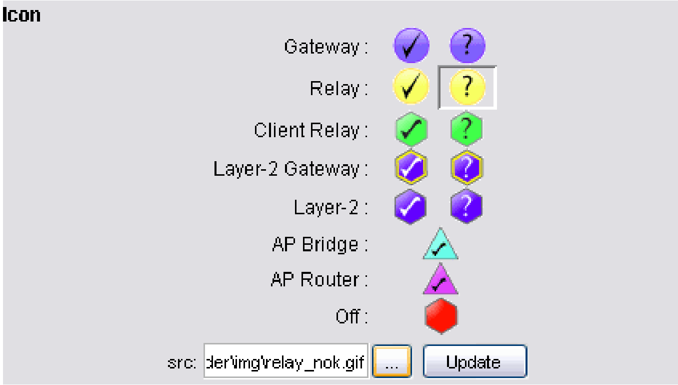
Pattern (line1, space1, line2, space2)	**Preview**
20, 0, 0, 0	
20, 10, 20, 10	
5, 10, 5, 10	
20, 3, 10, 3	
20, 10, 30, 5	

Here is an example to show the effect of the map customization.

a) The original map



b) Select Map Customization Tool and change the gateway & relay icon



Icon

Gateway : ✓ ?

Relay : ✓ ?

Client Relay : ✓ ?

Layer-2 Gateway : ✓ ?

Layer-2 : ✓ ?

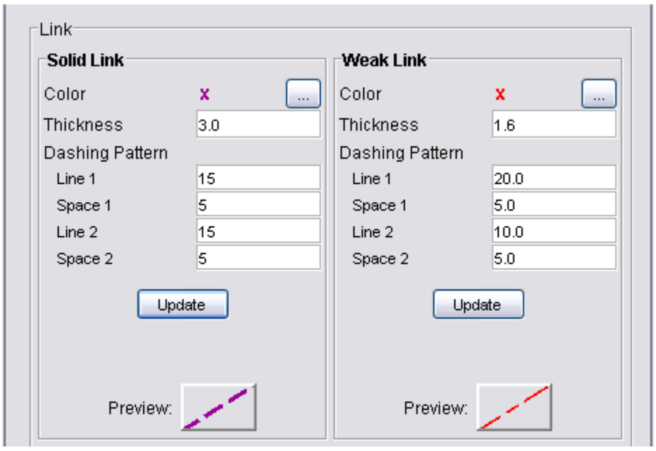
AP Bridge : ✓

AP Router : ✓

Off :

src: der\img\relay_nok.gif [...] [Update]

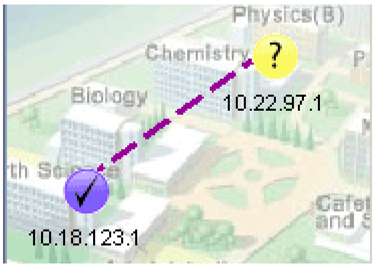
c) Switch to Link page and edit the attributes



Link

Solid Link		Weak Link	
Color	x [...]	Color	x [...]
Thickness	3.0	Thickness	1.6
Dashing Pattern		Dashing Pattern	
Line 1	15	Line 1	20.0
Space 1	5	Space 1	5.0
Line 2	15	Line 2	10.0
Space 2	5	Space 2	5.0
[Update]		[Update]	
Preview:		Preview:	

d) The customized map will look like this now.

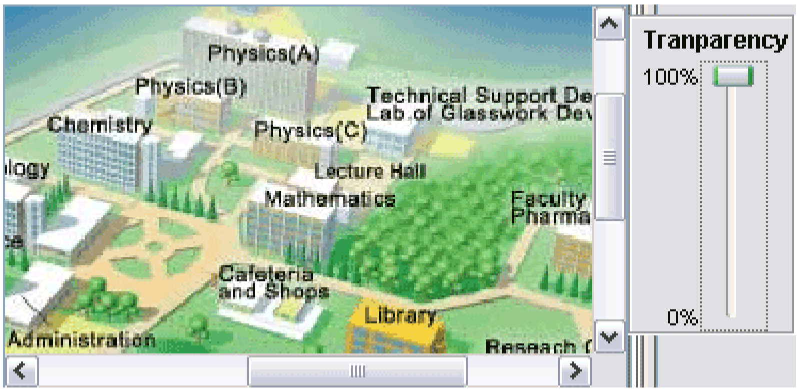


Note that, the changes of the AP unit node and link applies to every map created or opened on the NMS.

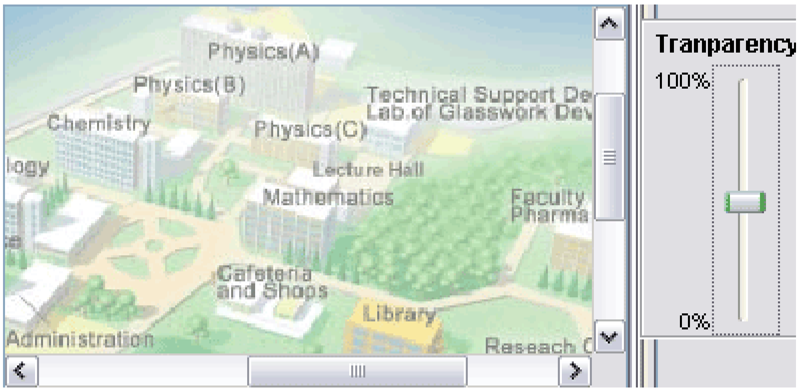
4.2.3.17 Background Image Transparency

This is a special tool used to adjust the opacity of the background image of the topology map. Select **Settings > Background Transparency** from the map container menu bar to allow users to alter the transparency of the background to a level that the APs and links are clear to view.

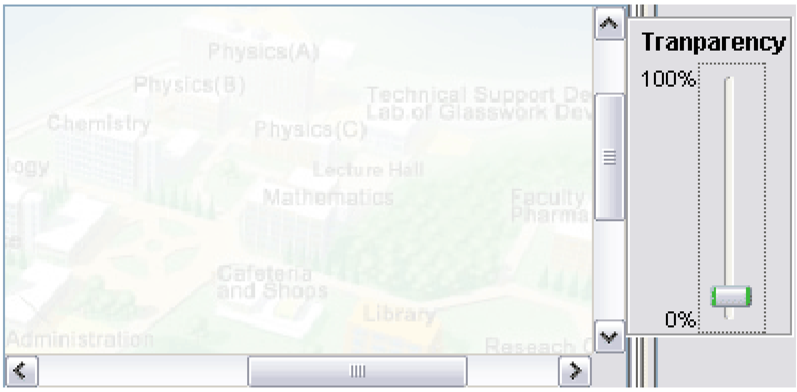
View the following figures to see the effect of the transparency tool.



(100%)



(50%)



(10%)

The tool will be closed automatically when it loses focus (mouse click anywhere out from the tool).

4.2.3.18 Block List

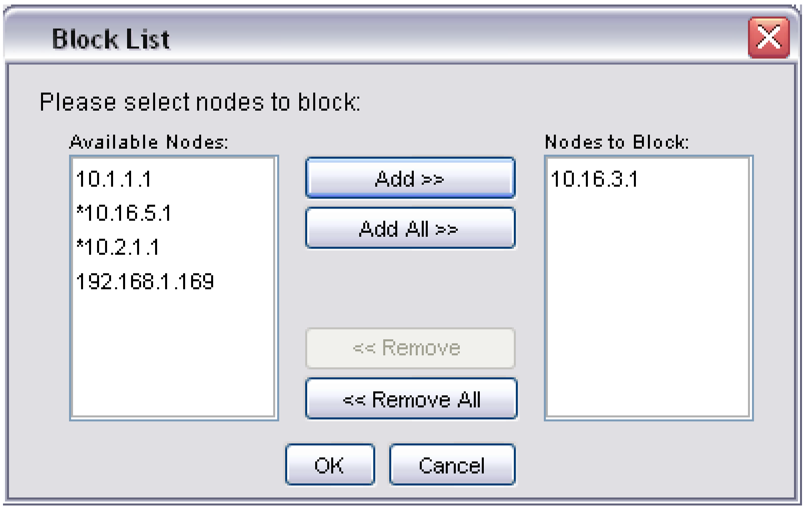
The Block List offers the NMS users a filtering tool in the topology map. User can define the IP Address to block, once the AP is blocked, it will be removed from the topology map, and will not be added to the map even if it is detected by the NMS.

To move an IP to the block list, click the **Block List** button on the toolbar, or select **Settings > Block List** from the menu bar. A window will emerge, as shown by the figure above. Then user can choose the node to block from the Available Nodes column. Select the IP, and hit the

Add button. The IP will be move over to the Nodes to Block column. On the other hand, if user wishes to undo the step, use the **Remove** button to move the IP back to the available list.

The **Add All** and **Remove All** button perform the same operation by moving every IPs in the list. Finally, hit the **OK** button to commit the change. (Note: asterisk in the list shows the IP is a gateway node).

The blocked IP Address will be saved into the map setting file when the user saves the topology map. Hence the IP will still be blocked when the current map profile reload in the future.

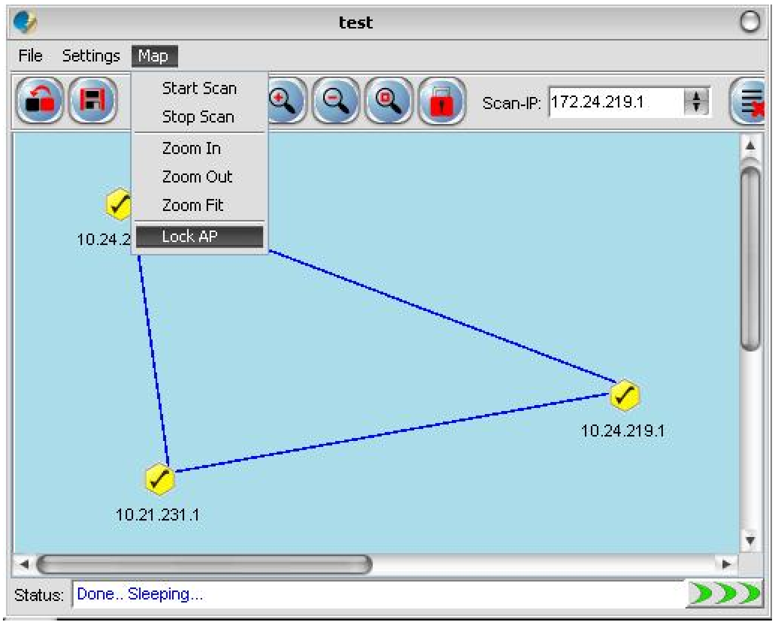


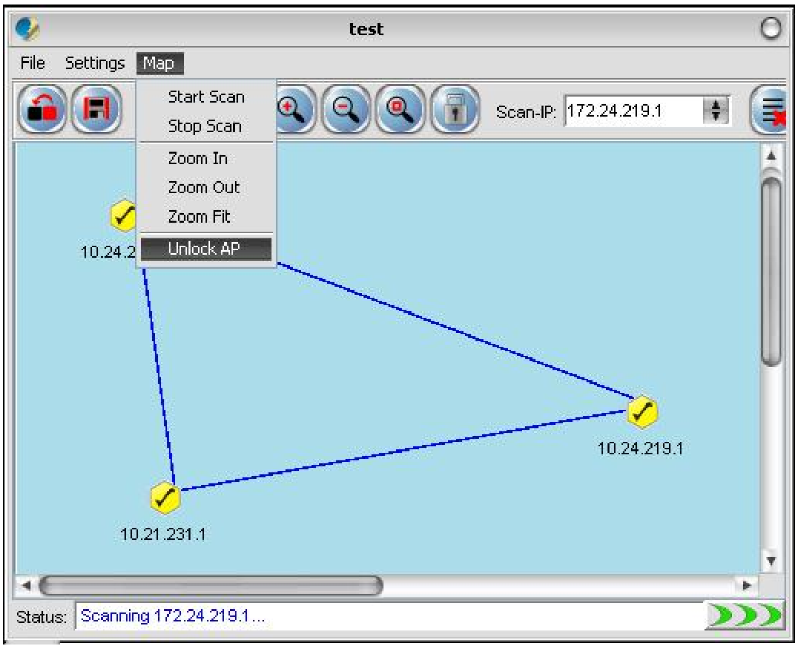
Available Nodes:
10.1.1.1
*10.16.5.1
*10.2.1.1
192.168.1.169

Nodes to Block:
10.16.3.1

4.2.3.19 Lock / Unlock

This feature is intended to prevent the user from dragging the node away from its current position accidentally. User can select **Map > Lock AP** from the menu bar or use the **Lock AP** button on the toolbar to lock up the nodes on the map.

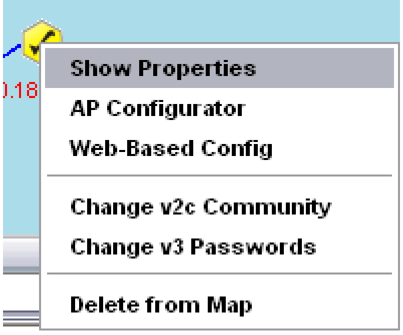


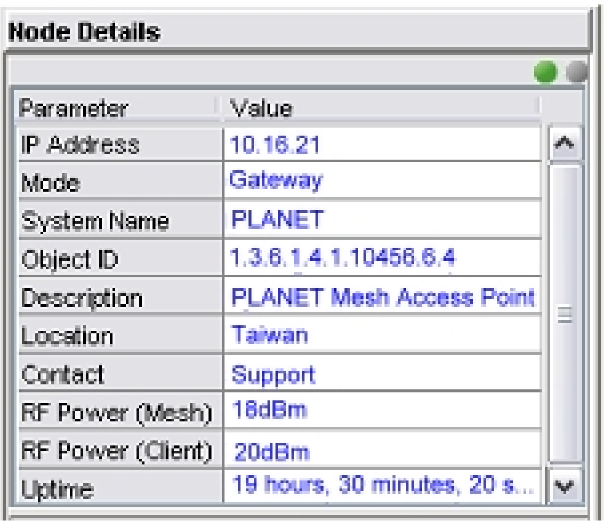


Conversely, click the **Map > Unlock AP** or **Unlock AP** button on the toolbar to release the lock. Hence, once user has complete positions the nodes, turn on the lock.

4.2.3.20 Node details

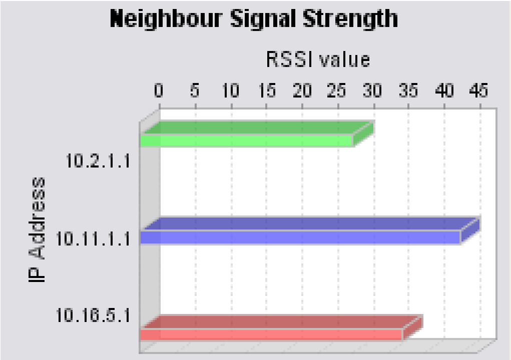
The table next to the map container is the node details table. The table displays the properties of the selected Mesh AP unit. In order to load the data, user can double-click on an active unit (gateway or relay or client-relay), or right click then choose the **Show Properties** item from the popup menu.




Node Details

Parameter	Value
IP Address	10.16.21
Mode	Gateway
System Name	PLANET
Object ID	1.3.6.1.4.1.10456.6.4
Description	PLANET Mesh Access Point
Location	Taiwan
Contact	Support
RF Power (Mesh)	18dBm
RF Power (Client)	20dBm
Uptime	19 hours, 30 minutes, 20 s...

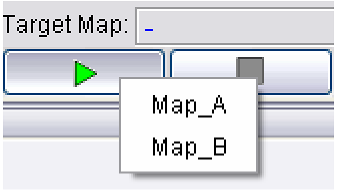
As mentioned previously, the NMS use the SNMP method to read the data. Hence if the data is failed to load, you may check the SNMP Community or Passwords. The two small circles on the top of the table indicate the status of the table. If the green circle is light up, it shows the table is loaded completely; if the orange circle is light up, it means the table is loading the data, else if the circle to turn to red color, it indicates that the data loading is failed.



On the other hand, the bar chart at the bottom of the table displaying the signal strength (in RSSI) between the selected AP and all its neighbour nodes. The scale of the chart can be enlarged by dragging the desired range of x-axis. Drag backward to reset the chart.

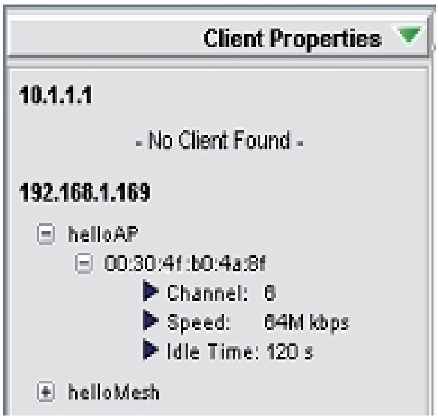
4.2.3.21 Client Properties

The client properties panel is located at the other side of the map container. In order to initiate the NMS to download the client details, hit on the **Start** button at the bottom of the panel. In case if there is more than one map is running, a menu would popup to prompt user to select which map to be targeted. Once selected, the scanning will be started instantly.



The automatic refresh feature of the client properties panel enable the admin uses the live information regarding the clients associated to the Mesh AP unit discovered by the NMS. The panel will be refreshed once per minute. On the other hand, if user wishes to refresh the panel manually, simply click the **Refresh** button at the bottom of the panel. While the downloading is in progress, the buttons will be replaced by a progress bar, showing the status of the process. The NMS will download the information from every single node in the target map discovered. To stop the scan, simply hit on the **Stop** button. The Target Map column displays the name of the map where the client panel is scanning.

The panel is divided into two portions, the Client Properties and Client Signal Strength. The Client Properties portion display the details regarding the client, for instance the MAC Address, channel number, link speed and the idle time. In the case if there is no client associated to the AP, a message “No Client Found” will be displayed instead.



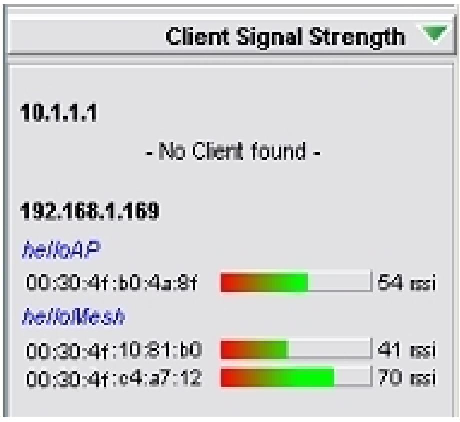
Client Properties

10.1.1.1

- No Client Found -

192.168.1.169

⊟ helloAP
  ⊟ 00:30:4f:b0:4a:8f
    ▶ Channel: 6
    ▶ Speed: 64M kbps
    ▶ Idle Time: 120 s
⊞ helloMesh



Client Signal Strength

10.1.1.1

- No Client found -

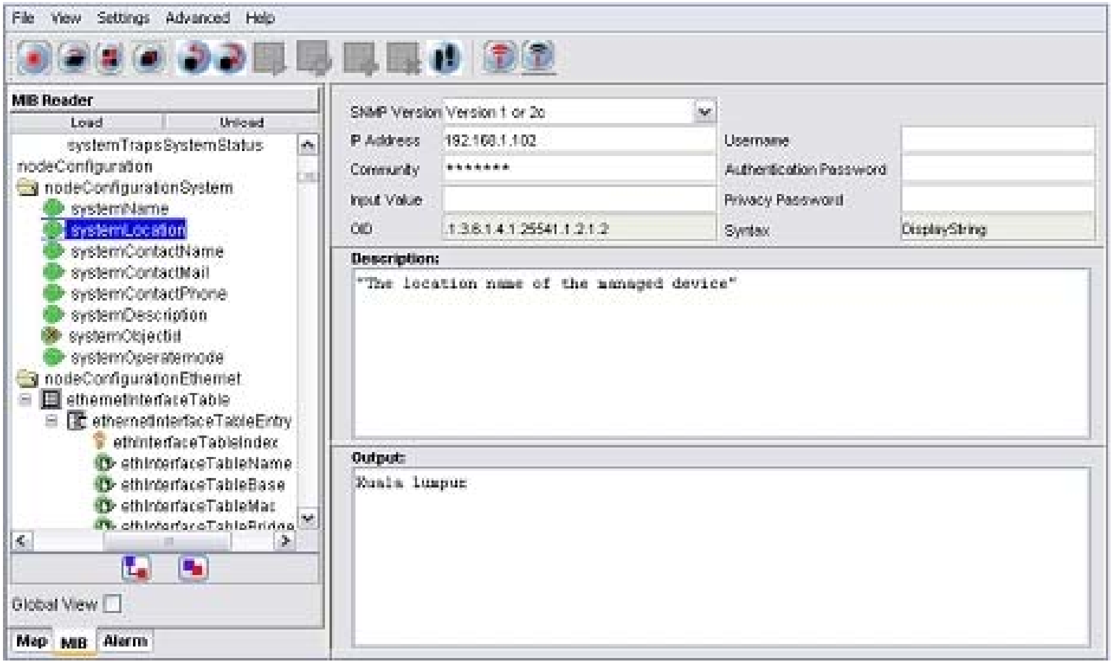
192.168.1.169

helloAP
00:30:4f:b0:4a:8f 54 rssi
helloMesh
00:30:4f:10:81:b0 41 rssi
00:30:4f:c4:a7:12 70 rssi

On the other hand, the Client Signal Strength panel displays the signal strength of the clients associated to the AP, in the unit of rssi. Similarly, if there is no client associated to the AP, a message “No Client Found” will be shown.

4.2.3.22 Get/Set using MIB Reader

This section describes briefly about the usage of the MIB Reader of the PLANET Mesh Network Management Tools.

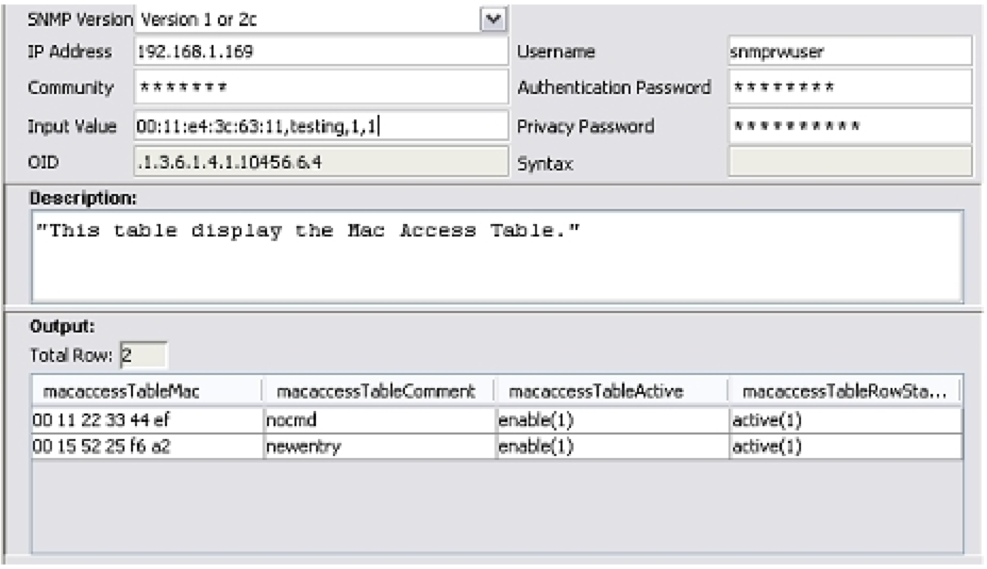


SNMP Version: Version 1 or 2c
IP Address: 192.168.1.102
Community: *******
Input Value:
OID: .1.3.6.1.4.1.25541.1.2.1.2
Username:
Authentication Password:
Privacy Password:
Syntax: DisplayString

Description:
"The location name of the managed device"

Output:
Kuala Lumpur

As illustrated, the center frame of the MIB Reader consists of three parts, SNMP keywords, description area and output area. The SNMP keywords portion is the area where user fills in the necessary parameter that need to perform any SNMP action. For instance, if the SNMP version to use is version 1 or 2c, then the Community is the required field; else if version 3 is selected, then user need to fill in the username, authentication password, and privacy password fields. The Input Value field is used when user wish to execute the SNMP Set command.



SNMP Version: Version 1 or 2c
IP Address: 192.168.1.169
Community: *******
Input Value: 00:11:e4:3c:63:11,testing,1,1
OID: .1.3.6.1.4.1.10456.6.4
Username: snmprwuser
Authentication Password: ********
Privacy Password: **********
Syntax:

Description:
"This table display the Mac Access Table."

Output:
Total Row: 2

macaccessTableMac	macaccessTableComment	macaccessTableActive	macaccessTableRowSta...
00 11 22 33 44 ef	nocmd	enable(1)	active(1)
00 15 52 25 f6 a2	newentry	enable(1)	active(1)

The Description area displays the description of the selected MIB tree node; whereas the Output area prints out the output of the SNMP action.

- **Get Action**

1. Select any tree node (make sure it is either read-only or read-write type)
2. Fill in the required parameter according to the version of SNMP to use.
3. Click the **SnmpGet** button on the toolbar.
4. The output should now display at the Output area.

- **Set Action**

1. Select any tree node (only read-write type)
2. Fill in the required parameter according to the version of SNMP to use.
3. Enter the value to be set at the Input Value column. You may refer the Syntax column to ensure the type of the input (eg: Integer, DisplayString..).
4. Click the **SnmpSet** button on the toolbar.
5. The Output area will display the result of the action, either "(Set Successfully…)" or "(Set Failed…)".

- **Read Table Action**

1. Select a table tree node
2. Fill in the required parameter according to the version of SNMP to use.
3. Click the **Load Table** button on the toolbar.
4. The Output field should display the whole table now.
5. Use the **Refresh Table** to reload the table.

- **Add Table Row Action**

1. Repeat the first three steps of Read Table Action
2. Then enter the table values in the Input Value field. Values are separated by a comma (,). (see the following figure)
3. Click the **Add Table Row** button on the toolbar.
4. The new entry should be added to the table.

- **Delete Table Row Action**

1. Repeat the first three steps of **Read Table Action**
2. Select the entry that you wish to remove from the table.
3. Click the **Delete Row** button on the toolbar.
4. A popup window would appear to ask for your confirmation to delete the selected entry. Hit **OK** to proceed.
5. The selected entry should be removed from the table.

- **Snmp Walk Action**

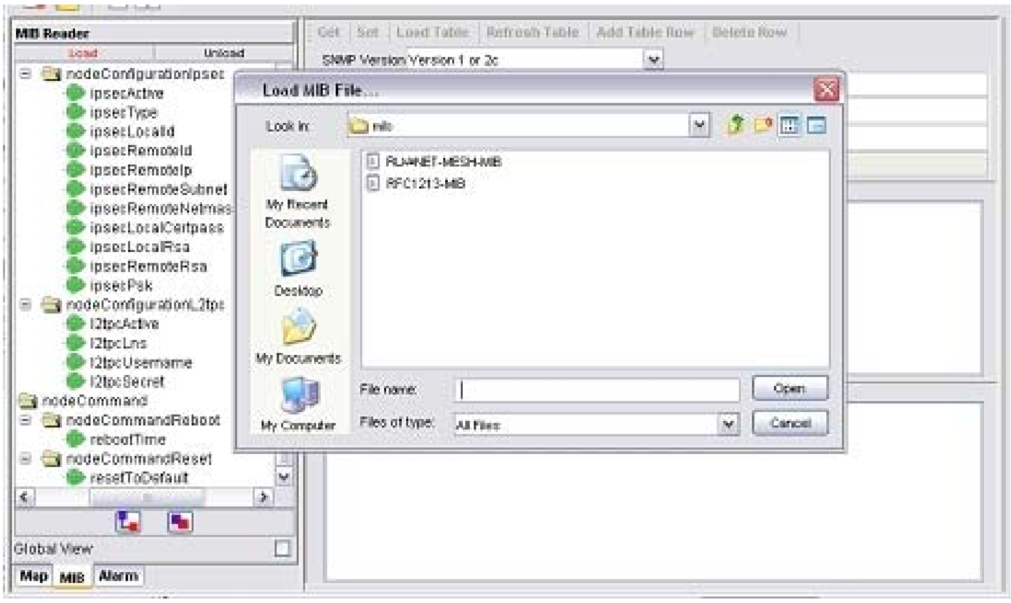
1. Select any tree node. (It can be a table, scalar or even the main node)
2. Fill in the required parameter according to the version of SNMP to use.

3. Click the **SnmpWalk** button on the toolbar.
4. The output should now display at the Output area. It could take some time to fetch all the data if the selected data is large.

Note: Please try to avoid Add or Delete the SNMP Table entry of the customized-MIB, since there are some tables which are internally correlated, such as VLAN table and Wireless table. Setting the table incorrectly would cause severe corruption in the system.

4.2.3.23 Load/Unload MIB

The MIB Reader of the NMS includes the feature to load and unload the MIB file from other resource. Therefore, instead of the customized MIB, user can load other standard MIB into the MIB Reader as well to read the parameter of the managed device.



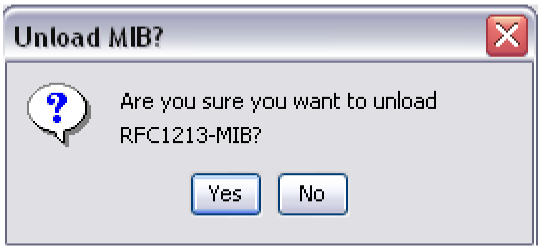
SNMP Version: Version 1 or 2c

Look in: mib

Files of type: All Files

In order to load a MIB, click on the **Load** button on the top of the MIB tree. A file chooser window would popup, to prompt user to enter the desired MIB file. Click **Open** to load the file.

On the other hand, the **Unload** button next to the **Load** button would unload the existing MIB in the tree. Select the unwanted MIB, click on the **Unload** button. A confirmation dialog box would turn up, to get confirmation from the user to remove the selected MIB. Click the **Yes** button to proceed.



Unload MIB?

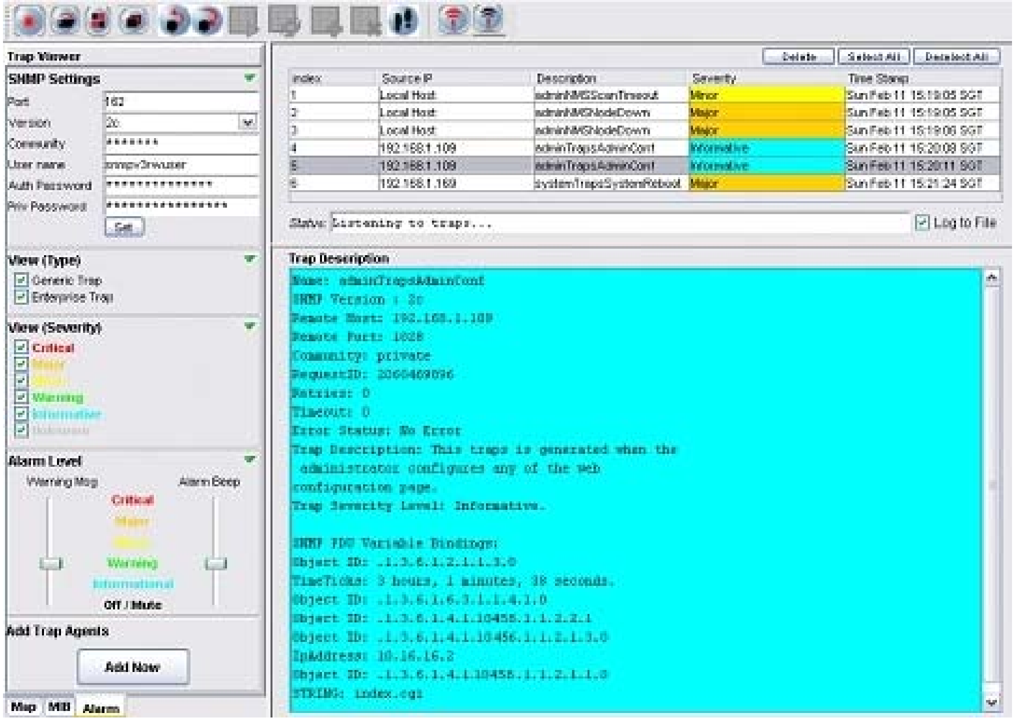
Are you sure you want to unload RFC1213-MIB?

4.2.3.24 Alarm Table

The Alarm Table of the PLANET Mesh Network Management Tools enable user to check on the traps and notifications caught by the trap receiver. The entries are read-only, and shall be deleted once they were resolved or reviewed.

In order to start listen to the traps, hit the **Start** button at the toolbar or select Settings > Start Trap from the menu bar. Select the **Stop** button, or Settings > Stop Trap to stop the trap listener. User can change the SNMP Trap community or passwords at the available columns and hit the **Set** button. The checkboxes at the bottom of the settings section are the table filtering options. Clear the selection of the checkbox to hide the relative entry in the trap table. Each level of severity is represented by a different color.

Select any entry from the alarm table, its description will be displayed at the Trap Description area at the bottom of the table. If you wish to remove the selected entry, click on the **Delete** button.



Trap Viewer

SNMP Settings

Port: 162
Version: 2c
Community: *******
User name: snmpv3rwuser
Auth Password: **************
Priv Password: ****************

View (Type)

☑ Generic Trap
☑ Enterprise Trap

View (Severity)

☑ Critical
☑ Major
☑ Minor
☑ Warning
☑ Informative
☑ Unknown

index	Source IP	Description	Severity	Time Stamp
1	Local Host	adminNMSScanTimeout	Minor	Sun Feb 11 15:19:05 SGT
2	Local Host	adminNMSNodeDown	Major	Sun Feb 11 15:19:05 SGT
3	Local Host	adminNMSNodeDown	Major	Sun Feb 11 15:19:06 SGT
4	192.168.1.109	adminTrapsAdminConf	Informative	Sun Feb 11 15:20:08 SGT
5	192.168.1.109	adminTrapsAdminConf	Informative	Sun Feb 11 15:20:11 SGT
6	192.168.1.169	systemTrapsSystemReboot	Major	Sun Feb 11 15:21:24 SGT

Status: Listening to traps...

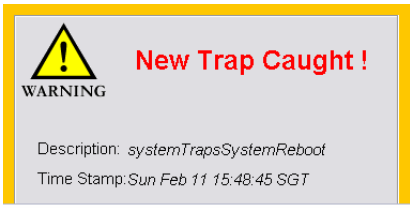
☑ Log to File

Trap Description

```
Name: adminTrapsAdminConf
SNMP Version : 2c
Remote Host: 192.168.1.109
Remote Port: 1028
Community: private
RequestID: 2060469096
Retries: 0
Timeout: 0
Error Status: No Error
Trap Description: This traps is generated when the
 administrator configures any of the web
configuration page.
Trap Severity Level: Informative.

SNMP PDU Variable Bindings:
Object ID: .1.3.6.1.2.1.1.3.0
TimeTicks: 3 hours, 1 minutes, 38 seconds.
Object ID: .1.3.6.1.6.3.1.1.4.1.0
Object ID: .1.3.6.1.4.1.10456.1.1.2.2.1
Object ID: .1.3.6.1.4.1.10456.1.1.2.1.3.0
IpAddress: 10.16.16.2
Object ID: .1.3.6.1.4.1.10456.1.1.2.1.1.0
STRING: index.cgi
```

The Alarm Level area is to enable the user to determine the level of the warning message popup and the alarm beep sound. User may drag the slider to alter the level. For instance, drag the slider of the warning message to Minor, the warning message would not popup if the level of the alarm received is Warning or Informational. The following figures illustrate the example of Warning Message, which will be displayed at the left bottom corner of the screen when the trap is received.



New Trap Caught !

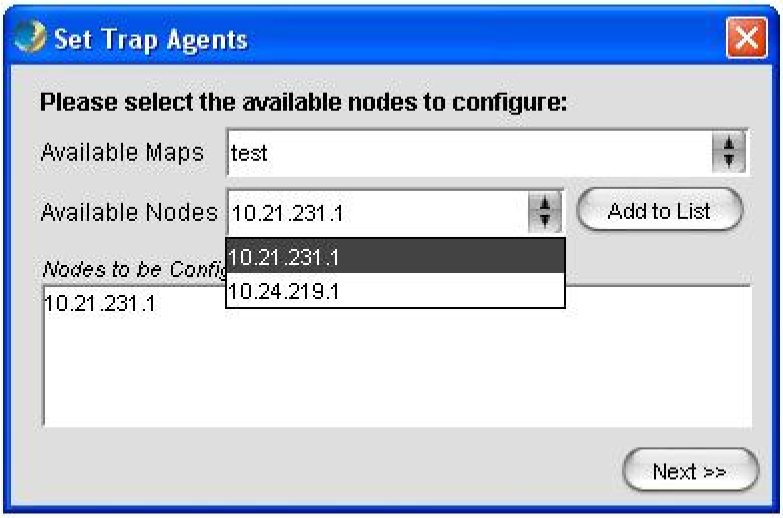
Description: systemTrapsSystemReboot

Time Stamp:Sun Feb 11 15:48:45 SGT

4.2.3.25 Add Trap Agent

This feature is a wizard window, intended to assist the user to set one, or more than one node to be the trap agent of the host system at the NMS, simultaneously.

Hit the **Add Now** button at the trap viewer mode, to invoke the wizard. At the first page of the wizard, user will be prompt to enter the IP Address of the desired nodes, to be set as alarm agent. User can enter the IP Address manually, or select from the drop down list provided. Click **Next** to proceed.



Set Trap Agents

Please select the available nodes to configure:

Available Maps: test

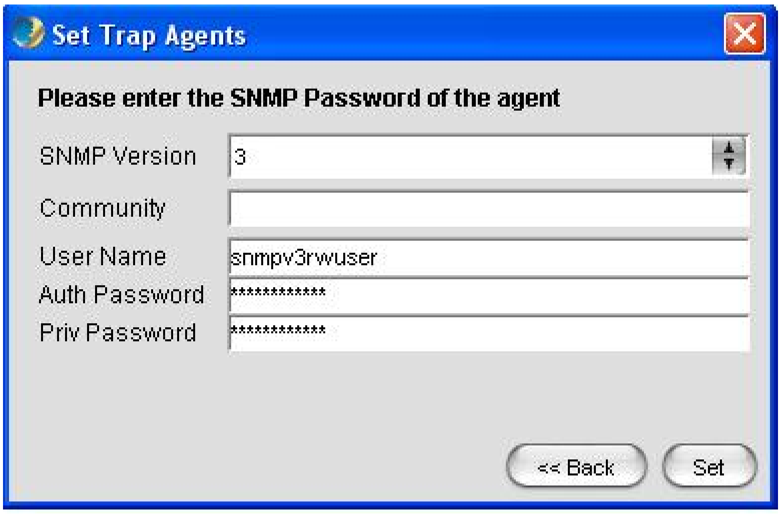
Available Nodes: 10.21.231.1

10.21.231.1
10.24.219.1

Nodes to be Confi

10.21.231.1

Then, enter the required SNMP keywords, such as version and community. Click **Set** to proceed or **Back** to back to the first step.



Please enter the SNMP Password of the agent

SNMP Version: 3

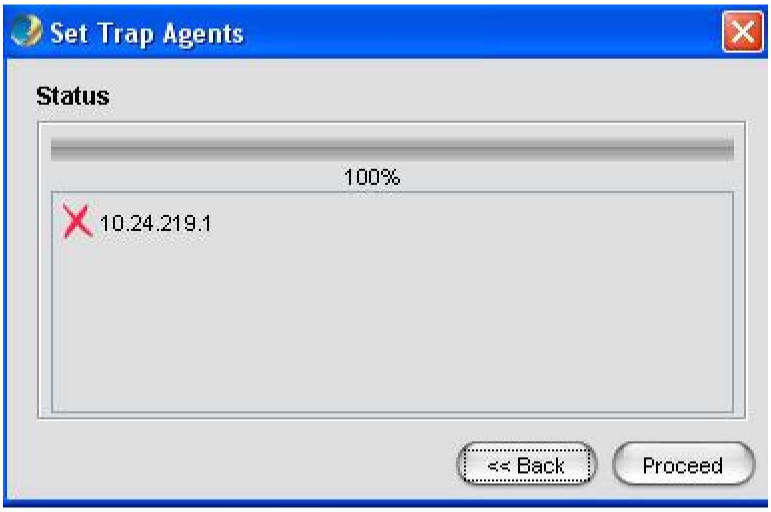
Community:

User Name: snmpv3rwuser

Auth Password: ************

Priv Password: ************

Once the configuration is done, click **Proceed** button to proceed to reboot page, or **Back** to the previous page.

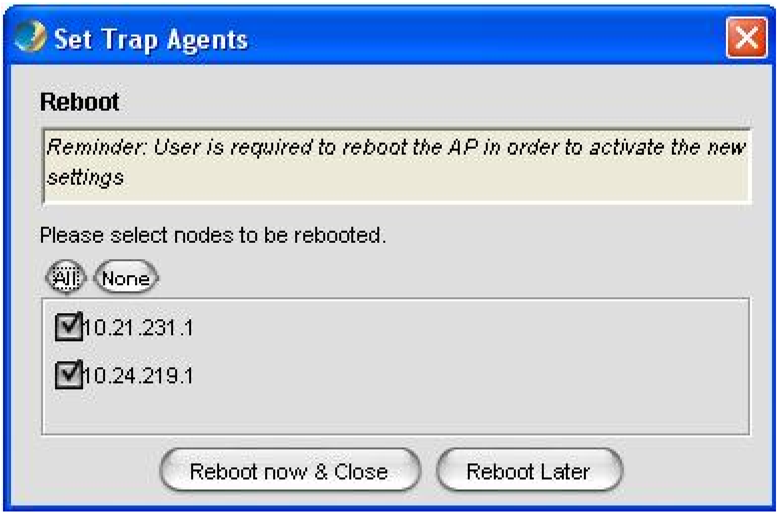


Status

100%

10.24.219.1

If **Proceed** is pressed, the following page will be displayed. User may select the IP Address of the node configured just now to be rebooted. In case if user is wished to reboot the device manually afterwards, click **Reboot Later**. On the other hand, hit the **Reboot now & Close** button to start reboot the devices.



Set Trap Agents

Reboot

Reminder: User is required to reboot the AP in order to activate the new settings

Please select nodes to be rebooted.

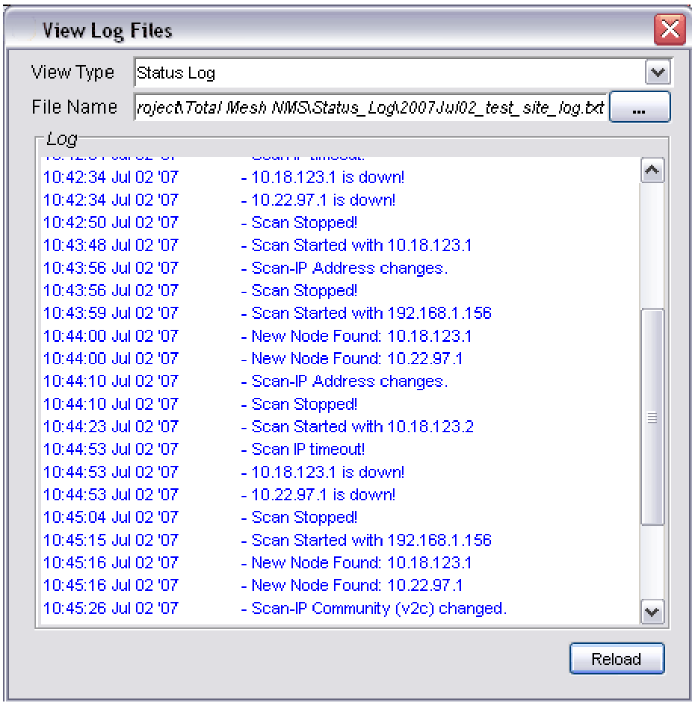
☑ 10.21.231.1

☑ 10.24.219.1

Once the AP unit is rebooted completely, it will contain the information of the Alarm Host System in the NMS. Hence, it will redirect the alarm message and notification to the NMS when there is any.

4.2.3.26 View Log Files

There is a feature in the NMS allow the user to back-track the log files of the system. Select **View > View Log** Files from the NMS menu bar to invoke a new dialog box, as shown at the following figures.



View Log Files

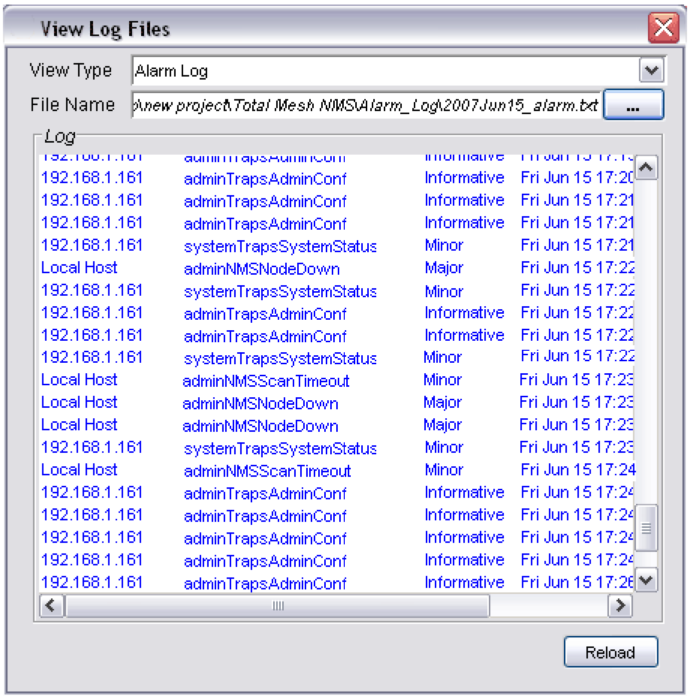
View Type: Status Log

File Name: *roject\Total Mesh NMS\Status_Log\2007Jul02_test_site_log.txt*

Log

```
10:42:34 Jul 02 '07     - 10.18.123.1 is down!
10:42:34 Jul 02 '07     - 10.22.97.1 is down!
10:42:50 Jul 02 '07     - Scan Stopped!
10:43:48 Jul 02 '07     - Scan Started with 10.18.123.1
10:43:56 Jul 02 '07     - Scan-IP Address changes.
10:43:56 Jul 02 '07     - Scan Stopped!
10:43:59 Jul 02 '07     - Scan Started with 192.168.1.156
10:44:00 Jul 02 '07     - New Node Found: 10.18.123.1
10:44:00 Jul 02 '07     - New Node Found: 10.22.97.1
10:44:10 Jul 02 '07     - Scan-IP Address changes.
10:44:10 Jul 02 '07     - Scan Stopped!
10:44:23 Jul 02 '07     - Scan Started with 10.18.123.2
10:44:53 Jul 02 '07     - Scan IP timeout!
10:44:53 Jul 02 '07     - 10.18.123.1 is down!
10:44:53 Jul 02 '07     - 10.22.97.1 is down!
10:45:04 Jul 02 '07     - Scan Stopped!
10:45:15 Jul 02 '07     - Scan Started with 192.168.1.156
10:45:16 Jul 02 '07     - New Node Found: 10.18.123.1
10:45:16 Jul 02 '07     - New Node Found: 10.22.97.1
10:45:26 Jul 02 '07     - Scan-IP Community (v2c) changed.
```

Then user can select the type of log to view, including Status Log and Alarm Log. Key in the desired file name, or hit the button next to the column to select the file, and select the **Reload** button to load the content of the file.



View Type: Alarm Log

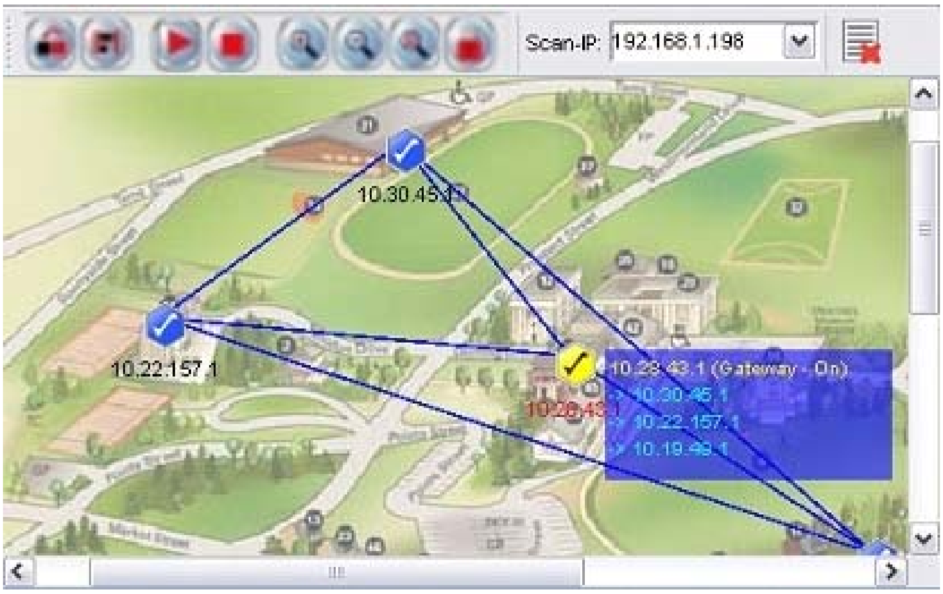
File Name: \new project\Total Mesh NMS\Alarm_Log\2007Jun15_alarm.txt

Log

```
192.168.1.161   adminTrapsAdminConf        Informative  Fri Jun 15 17:1
192.168.1.161   adminTrapsAdminConf        Informative  Fri Jun 15 17:20
192.168.1.161   adminTrapsAdminConf        Informative  Fri Jun 15 17:21
192.168.1.161   adminTrapsAdminConf        Informative  Fri Jun 15 17:21
192.168.1.161   systemTrapsSystemStatus    Minor        Fri Jun 15 17:21
Local Host      adminNMSNodeDown           Major        Fri Jun 15 17:22
192.168.1.161   systemTrapsSystemStatus    Minor        Fri Jun 15 17:22
192.168.1.161   adminTrapsAdminConf        Informative  Fri Jun 15 17:22
192.168.1.161   adminTrapsAdminConf        Informative  Fri Jun 15 17:22
192.168.1.161   systemTrapsSystemStatus    Minor        Fri Jun 15 17:22
Local Host      adminNMSScanTimeout        Minor        Fri Jun 15 17:23
Local Host      adminNMSNodeDown           Major        Fri Jun 15 17:23
Local Host      adminNMSNodeDown           Major        Fri Jun 15 17:23
192.168.1.161   systemTrapsSystemStatus    Minor        Fri Jun 15 17:23
Local Host      adminNMSScanTimeout        Minor        Fri Jun 15 17:24
192.168.1.161   adminTrapsAdminConf        Informative  Fri Jun 15 17:24
192.168.1.161   adminTrapsAdminConf        Informative  Fri Jun 15 17:24
192.168.1.161   adminTrapsAdminConf        Informative  Fri Jun 15 17:24
192.168.1.161   adminTrapsAdminConf        Informative  Fri Jun 15 17:24
192.168.1.161   adminTrapsAdminConf        Informative  Fri Jun 15 17:26
```

4.2.3.27 Show Route

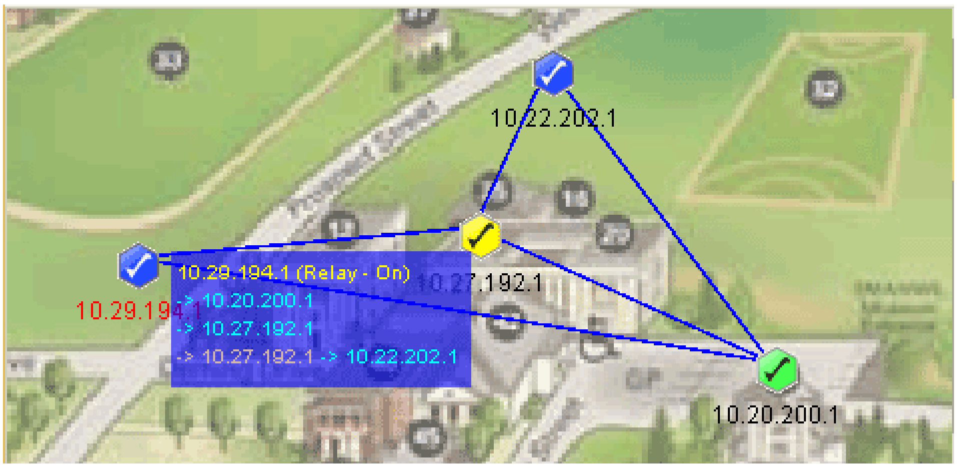
When user moves the mouse over the plotted AP unit on the topology map, a small blue dialog would appear on the screen, displaying the routes of the selected unit. The route describes how the AP link to the other nodes in the same mesh network, as illustrated by the figure below.



Scan-IP: 192.168.1.198

10.28.43.1 (Gateway - On)
-> 10.30.45.1
-> 10.22.157.1
-> 10.19.49.1

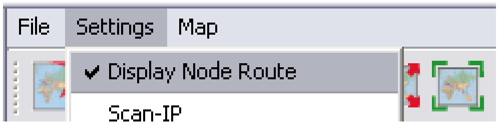
The figure above shows the node 10.28.43.1 is currently connected directly to 10.30.45.1, 10.22.157.1, and 10.19.49.1.



10.29.194.1 (Relay - On)
-> 10.20.200.1
-> 10.27.192.1
-> 10.27.192.1 -> 10.22.202.1

Whereas the figure above illustrates how the routes are displayed when nodes are not directly connected. From the example, node 10.29.194.1 and 10.22.202.1 are not directly connected. Instead, the connection between them is established via node 10.27.192.1, according to the route box.

If user would like to disable this feature, please select **Settings > Display Node Route** from the map container menu bar.

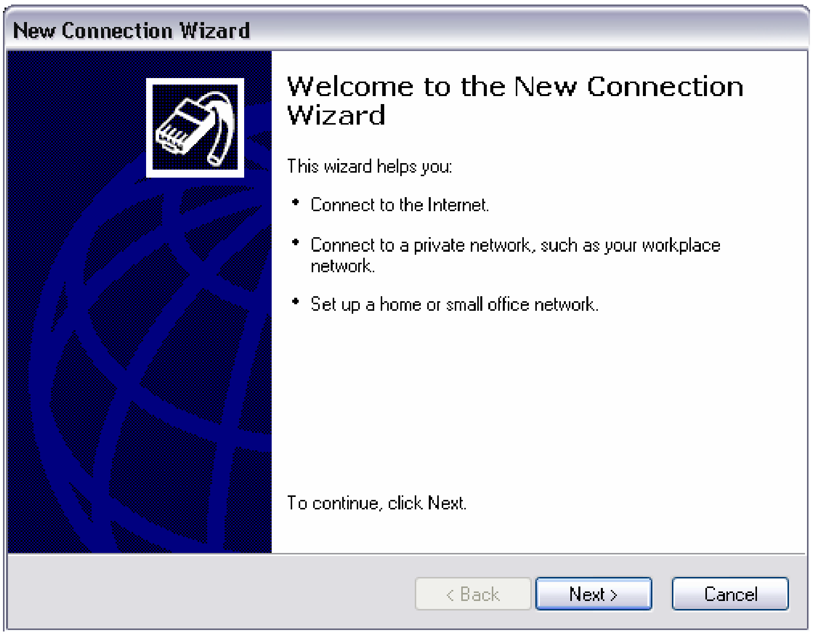


4.2.3.28 Create VPN Connection

If user would like to scan a network through the backbone line (WAN), a VPN Connection is required in order to create the communication link between the NMS and the Mesh APs discovered through a VPN Server.

To create a new VPN Connection, use the **New Connection wizard** of Windows. In order to start-up the wizard, open the Network Connections Page (**Start Menu > Control Panel > Network Connections**), then select **New Connection Wizard**. When the wizard turn up, follow the following steps to do the set up: (*refer to the following screen shots)

- Introduction – Welcome page of the wizard



New Connection Wizard

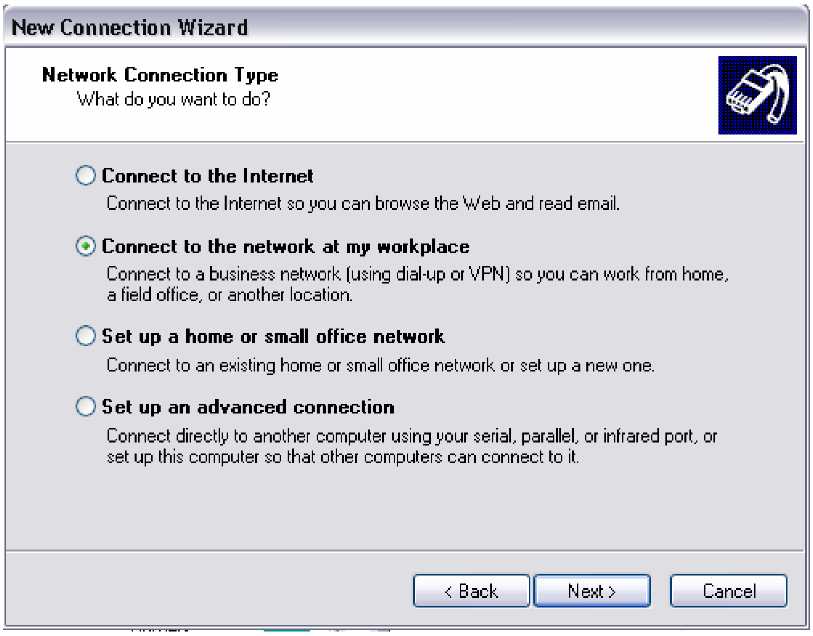
Welcome to the New Connection Wizard

This wizard helps you:

- Connect to the Internet.
- Connect to a private network, such as your workplace network.
- Set up a home or small office network.

To continue, click Next.

- Network Connection Type – Select **Connect to the network at my workplace** and click **Next** button



New Connection Wizard

Network Connection Type
What do you want to do?

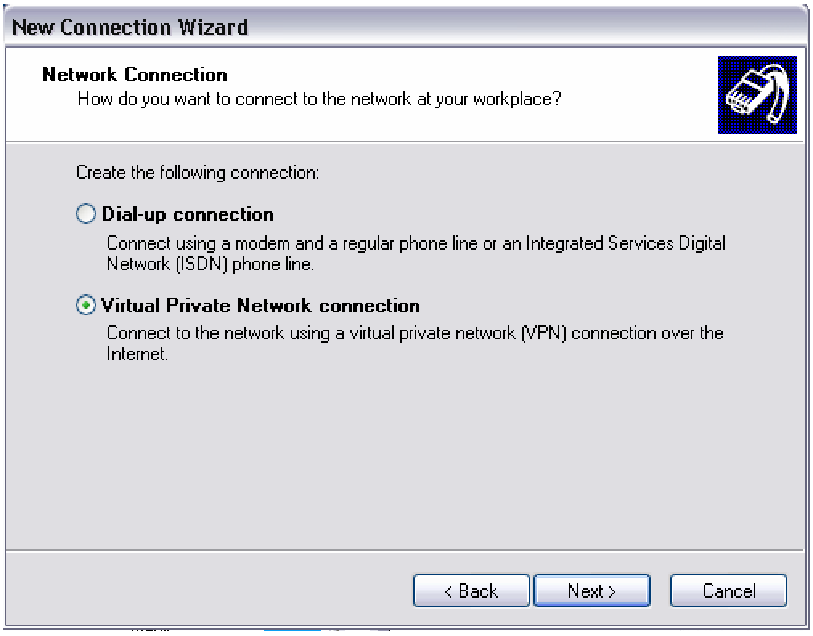
○ **Connect to the Internet**
Connect to the Internet so you can browse the Web and read email.

● **Connect to the network at my workplace**
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

○ **Set up a home or small office network**
Connect to an existing home or small office network or set up a new one.

○ **Set up an advanced connection**
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

- Network Connection – Select **Virtual Private Network** and click the **Next** button



New Connection Wizard

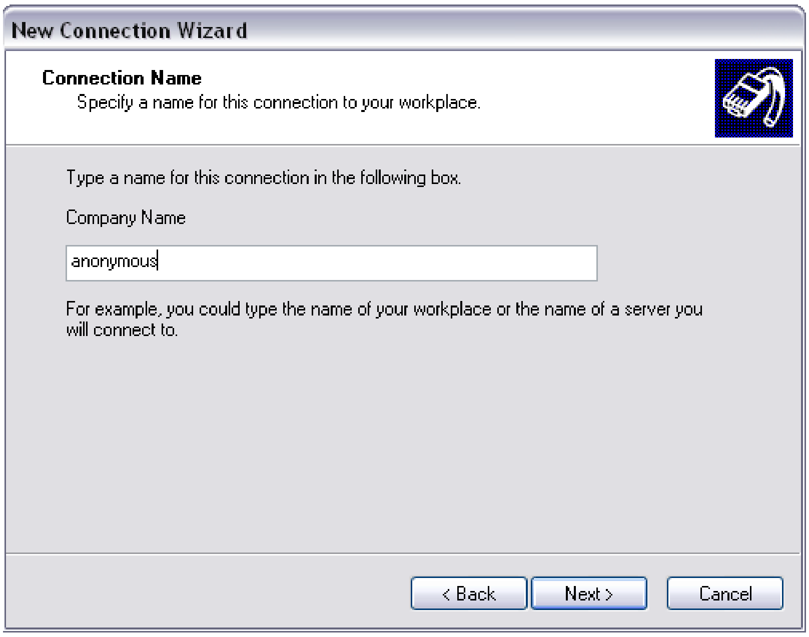
Network Connection
How do you want to connect to the network at your workplace?

Create the following connection:

○ **Dial-up connection**
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.

● **Virtual Private Network connection**
Connect to the network using a virtual private network (VPN) connection over the Internet.

- Connection Name – Enter a desired Connection Name and hit the **Next** button



New Connection Wizard

Connection Name

Specify a name for this connection to your workplace.

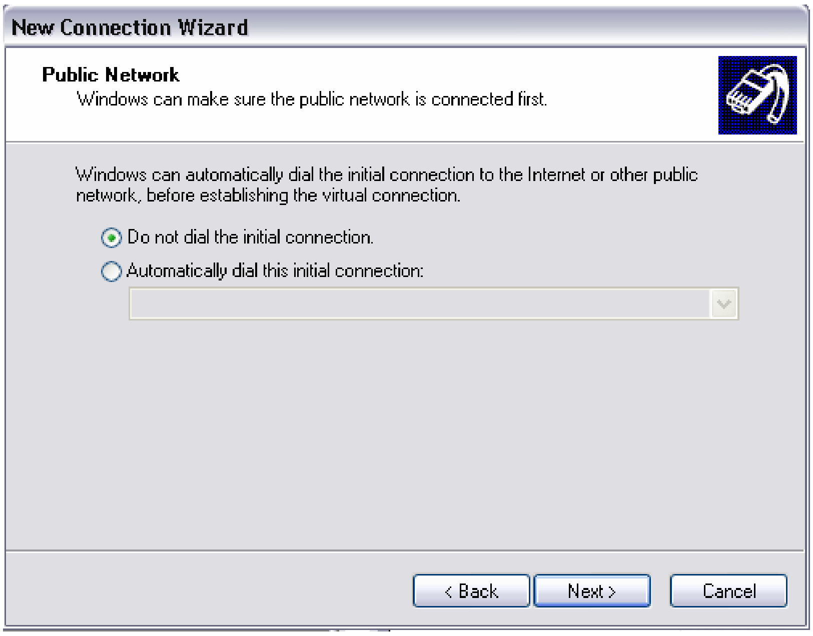
Type a name for this connection in the following box.

Company Name

anonymous

For example, you could type the name of your workplace or the name of a server you will connect to.

- Public Network – Select **Do not dial initial connection** and press **Next** button



New Connection Wizard

Public Network

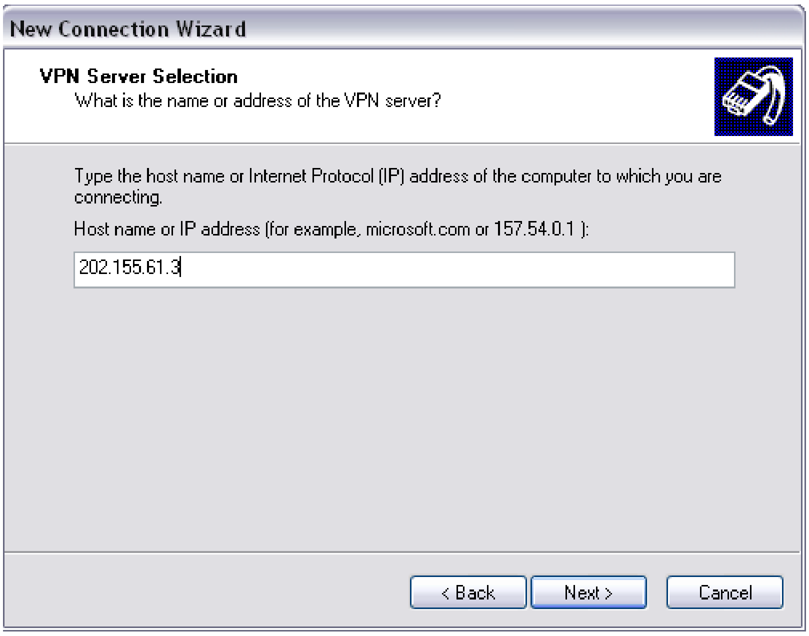
Windows can make sure the public network is connected first.

Windows can automatically dial the initial connection to the Internet or other public network, before establishing the virtual connection.

● Do not dial the initial connection.

○ Automatically dial this initial connection:

- VPN Server Selection – Enter the host name or the IP Address of the VPN Server that you wish to connect, and click the **Next** button



New Connection Wizard

VPN Server Selection
What is the name or address of the VPN server?

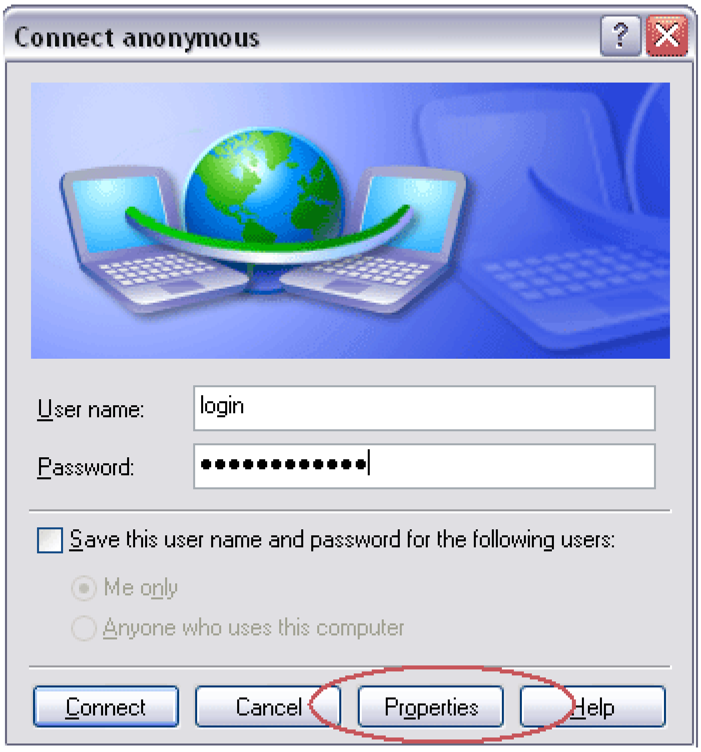
Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.

Host name or IP address (for example, microsoft.com or 157.54.0.1):

202.155.61.3

- Complete – Click **Finish** to complete the set up

After the shortcut is created, user is required to go to the **Properties** page, by right-click on the shortcut icon, and then choose from the popup menu. Alternatively, it can be opened from the Connect page, as shown:



Connect anonymous

User name: login

Password: ●●●●●●●●●●●●●

□ Save this user name and password for the following users:

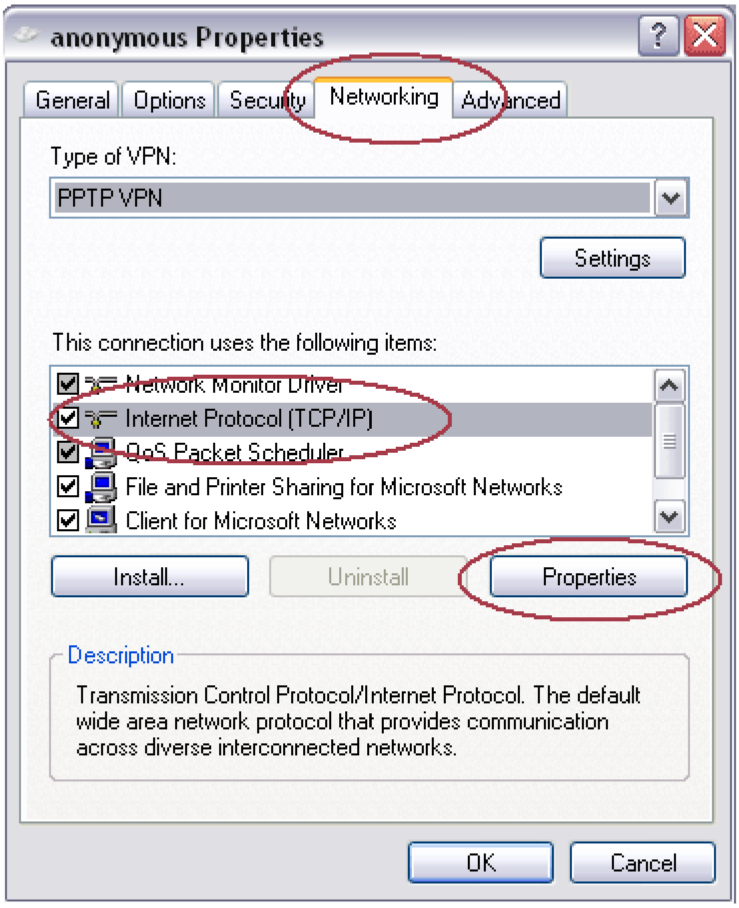
● Me only

○ Anyone who uses this computer

At the Connection Properties window, perform the following steps:

- Select the Networking Tab at the top of the page
- Select **PPTP VPN** in the Type of VPN field.
- Select the Internet Protocol (TCP/IP) from the available list

- Hit the **Properties** button to configure the item's properties
- At the TCP/IP Properties window, select the **Advanced..** button, another window (Advanced TCP/IP Settings) would appear.
- At this window, make sure the Use default gateway on remote network option is checked and click the **OK** button.



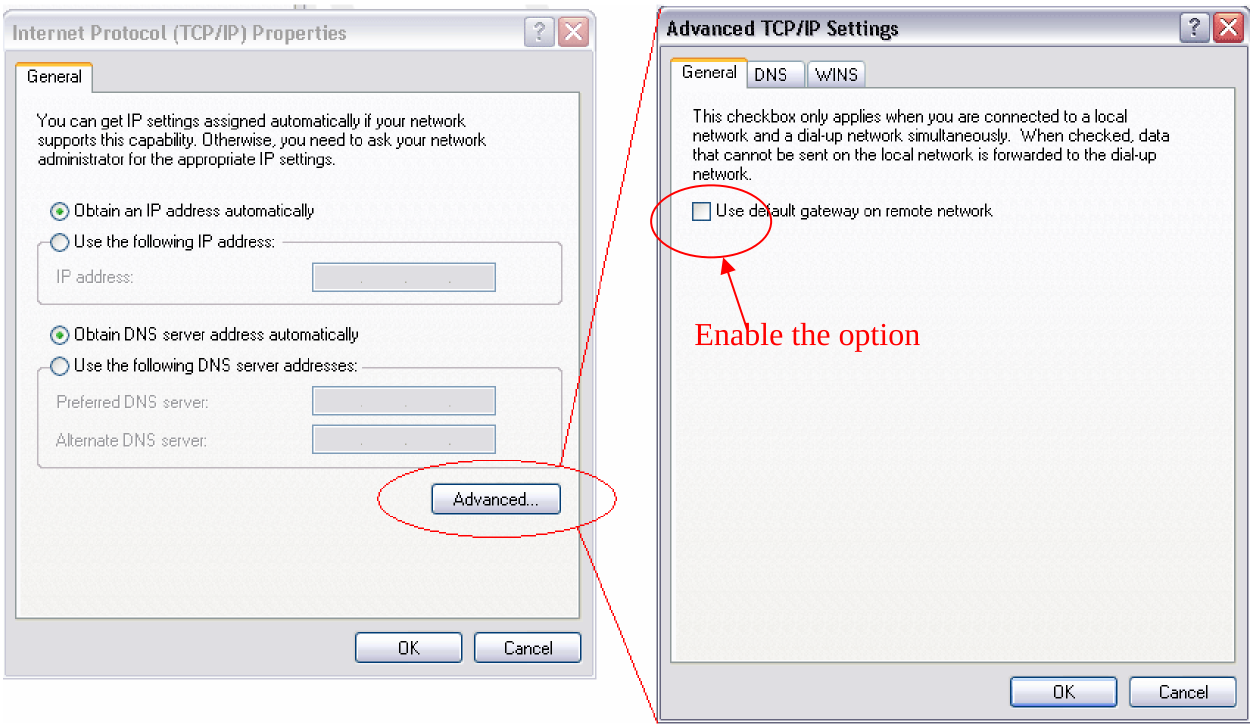
Type of VPN: PPTP VPN

This connection uses the following items:

☑ Network Monitor Driver
☑ Internet Protocol (TCP/IP)
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Client for Microsoft Networks

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

Advanced TCP/IP Settings

This checkbox only applies when you are connected to a local network and a dial-up network simultaneously. When checked, data that cannot be sent on the local network is forwarded to the dial-up network.

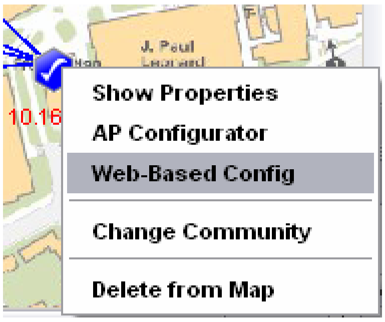
□ Use default gateway on remote network

Enable the option

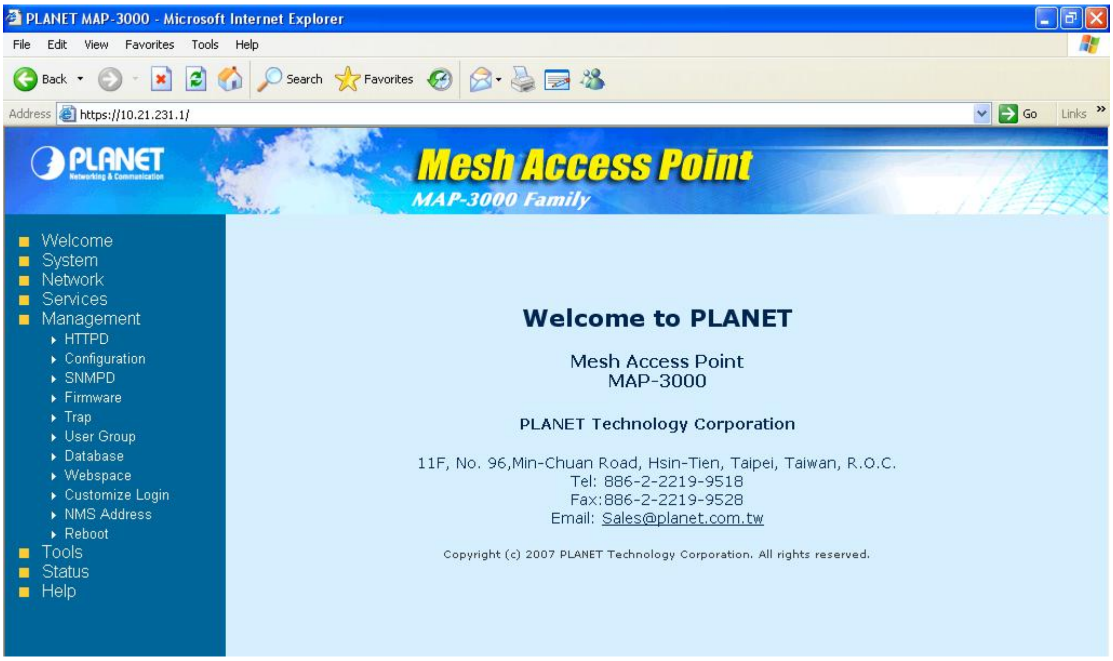
The configuration of the VPN is done.

4.2.3.29 Configure Mesh APs

Two methods are available to configure the Mesh AP unit remotely via the NMS,: thru Web-based Configuration Page or launch the AP Configurator. In order to invoke any of these two methods, right click on any of the active Mesh AP unit on the topology map (gateway or relay). A popup menu would appear, as shown:



Select the **AP Configurator** or **Web-Based Config** option. The following figure shows the screenshot of the Web-based Configuration page.



Welcome to PLANET

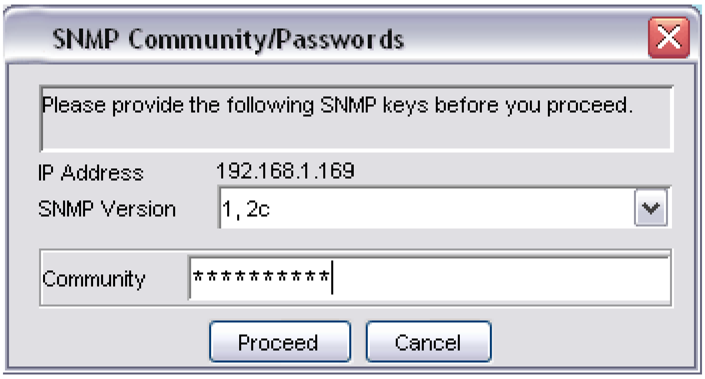
Mesh Access Point
MAP-3000

PLANET Technology Corporation

11F, No. 96,Min-Chuan Road, Hsin-Tien, Taipei, Taiwan, R.O.C.
Tel: 886-2-2219-9518
Fax:886-2-2219-9528
Email: Sales@planet.com.tw

Copyright (c) 2007 PLANET Technology Corporation. All rights reserved.

If the AP Configurator is selected instead, a window would appear to prompt user for the SNMP password and community, as shown:


SNMP Community/Passwords

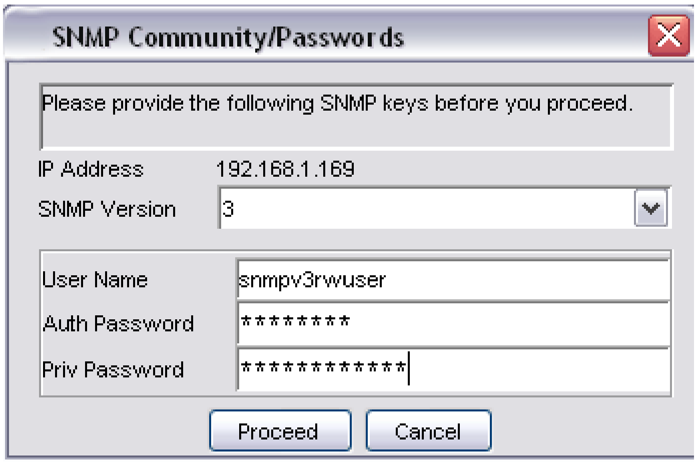
Please provide the following SNMP keys before you proceed.

IP Address 192.168.1.169

SNMP Version 1, 2c

Community **********

(Version 1 and 2C)


SNMP Community/Passwords

Please provide the following SNMP keys before you proceed.

IP Address 192.168.1.169

SNMP Version 3

User Name snmpv3rwuser

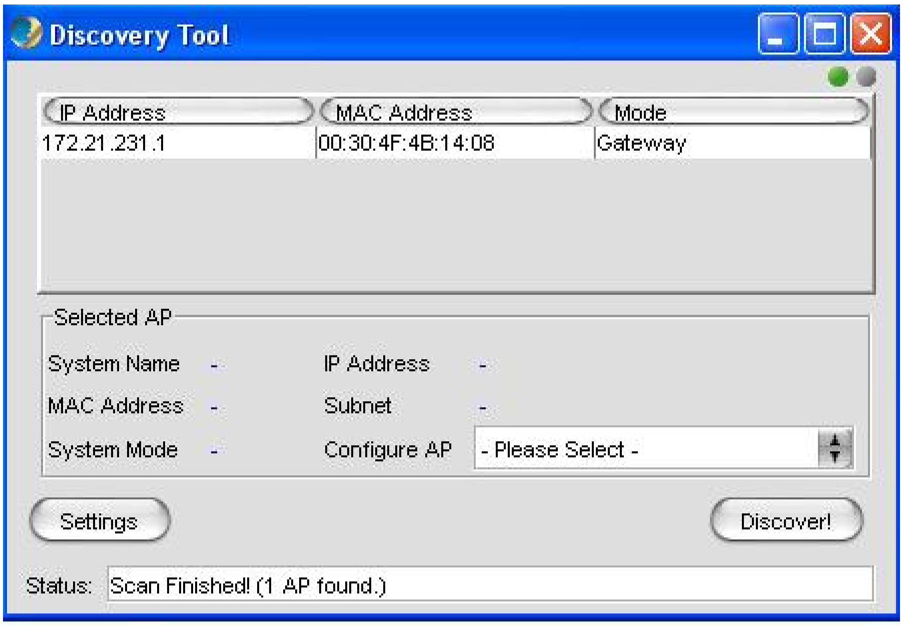
Auth Password ********

Priv Password ************

(Version 3)

After enter the required passwords, click the **Proceed** button to initiate the AP Configurator. If the password is incorrect, an error message will show on the screen and urge user to reenter the password accurately. For more details regarding the AP Configurator, please refer to the next section.

4.2.3.30 Discovery Tool



IP Address	MAC Address	Mode
172.21.231.1	00:30:4F:4B:14:08	Gateway

Selected AP

System Name	-	IP Address	-
MAC Address	-	Subnet	-
System Mode	-	Configure AP	- Please Select -

Status: Scan Finished! (1 AP found.)

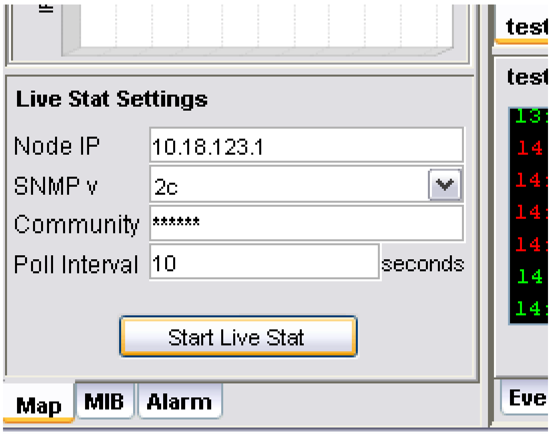
The discovery tool is an advance feature added to the NMS. Its main function is used to discover the recognized AP unit locating in the same subnet. Hit the **Discover** button at the bottom to initiate the scan. The APs found throughout the process will be displayed on the table.

User may click on the entry on the table to view the information regarding the AP, such as system name, MAC address and so forth. Further more, the selected unit can be configured by using the drop-down list at the top of the **Discover** button, to open the AP-Configurator or Web-based configuration page.

4.2.3.31 View Interface and Client Live Statistic

The new feature added in the latest version of NMS, provides user a graphical and readable statistic table regarding the target Mesh AP unit. The information that monitored by the live stat portion includes the interfaces throughput, clients’ throughput, as well as the memory status.

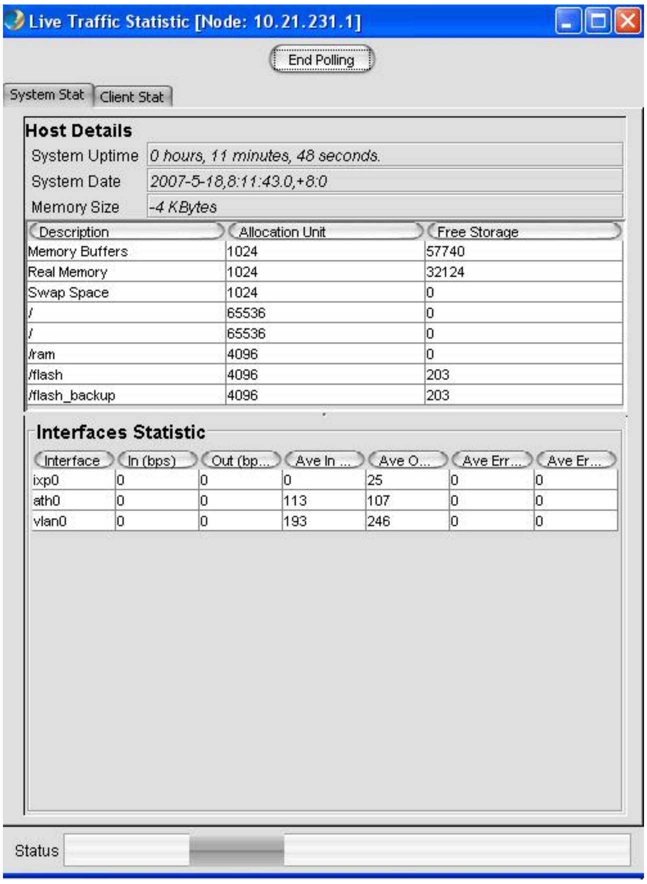
In order to invoke the live stat window, switch the NMS to the Map Container view, and then look for the Live Stat Settings portion at the left bottom corner. User may enter the IP Address of the target node (or just click on the node on the map to load the IP) to be monitored, and its corresponding SNMP Key. Hit the **Start Live Stat** button to initiate the window.



Live Stat Settings

Node IP: 10.18.123.1
SNMP v: 2c
Community: ******
Poll Interval: 10 seconds

At the popup live stat window, click the **Start Polling** button at the top to start the live stat. The window consists of two parts: the System Stat and the Client Stat. The System Stat page displays the memory status of the system and the statistic of the interfaces throughput. The table will be updated at a certain interval, which is set by the Poll Interval field at the Live Stat Settings corner.



Live Traffic Statistic [Node: 10.21.231.1]

Host Details

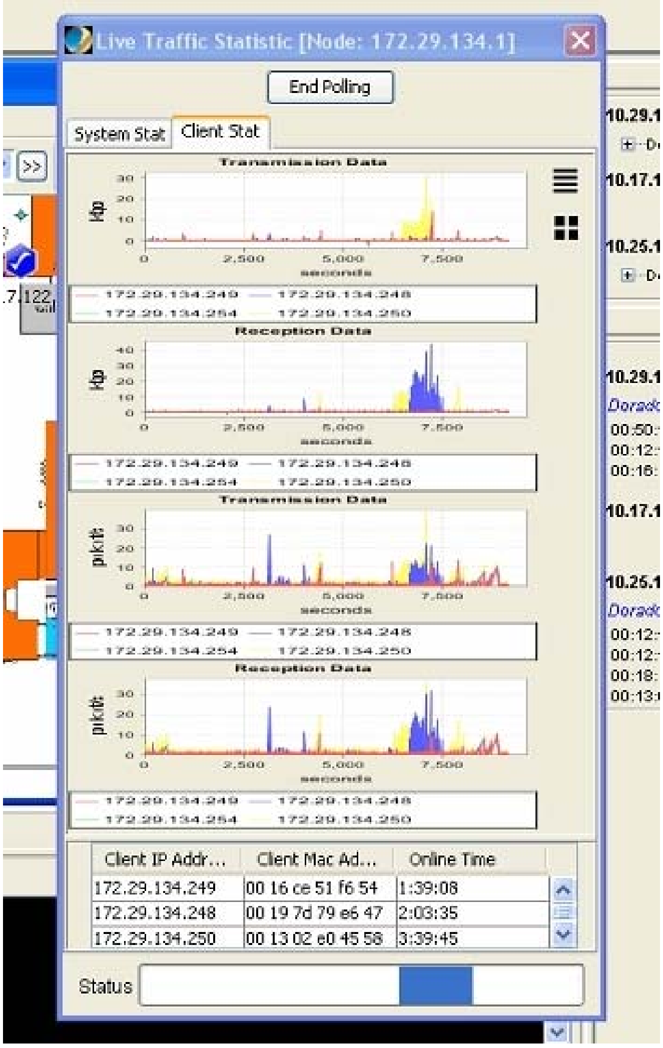
System Uptime: 0 hours, 11 minutes, 48 seconds.
System Date: 2007-5-18,8:11:43.0,+8:0
Memory Size: -4 KBytes

Description	Allocation Unit	Free Storage
Memory Buffers	1024	57740
Real Memory	1024	32124
Swap Space	1024	0
/	65536	0
/	65536	0
/ram	4096	0
/flash	4096	203
/flash_backup	4096	203

Interfaces Statistic

Interface	In (bps)	Out (bp...	Ave In ...	Ave O...	Ave Err...	Ave Er...
ixp0	0	0	0	25	0	0
ath0	0	0	113	107	0	0
vlan0	0	0	193	246	0	0

The second page shows the throughput statistic of every client that associated to target node. The results of the transmission and reception data packet rate are displayed in the form of graph. The table at the bottom of the graphs tabulates the client list with their respective MAC Address and online time. To stop the polling process, click the **End Polling** button at the top.

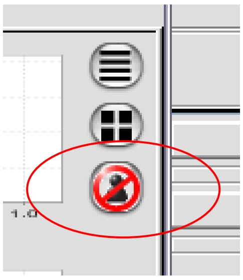


Client IP Addr...	Client Mac Ad...	Online Time
172.29.134.249	00 16 ce 51 f6 54	1:39:08
172.29.134.248	00 19 7d 79 e6 47	2:03:35
172.29.134.250	00 13 02 e0 45 58	3:39:45

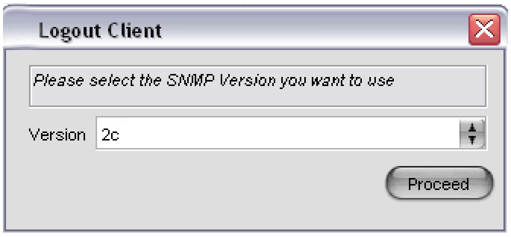
4.2.3.32   Logout Client

With the NMS, the administrator is able to log out and block the user from accessing the network, by using the **Logout and Block user** button at the Live Stat Window

In order to remove the client, user must run the Live Stat Window. In the Client Stat portion, the table at the bottom lists the client that has log on to the network. Select the client (Mac Address) that to be removed, and hit the **Logout and Block user** button.



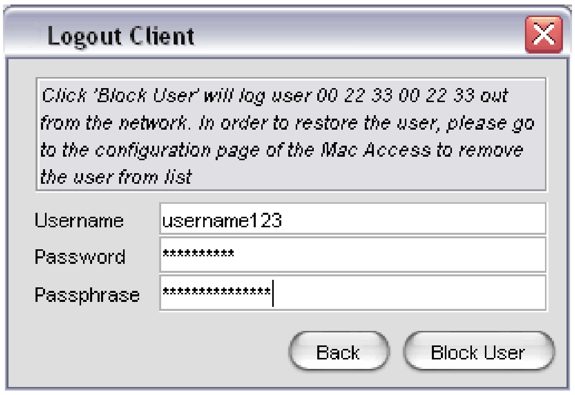
A window would appear on the screen to prompt user for the SNMP version to use and its corresponding community or passwords. Click the **Block User** button once completed the step, the selected client will be removed from the active client table, and added into the MAC Access Table.



Logout Client

Please select the SNMP Version you want to use

Version: 2c



Logout Client

Click 'Block User' will log user 00 22 33 00 22 33 out from the network. In order to restore the user, please go to the configuration page of the Mac Access to remove the user from list

Username: username123

Password: **********

Passphrase: ***************

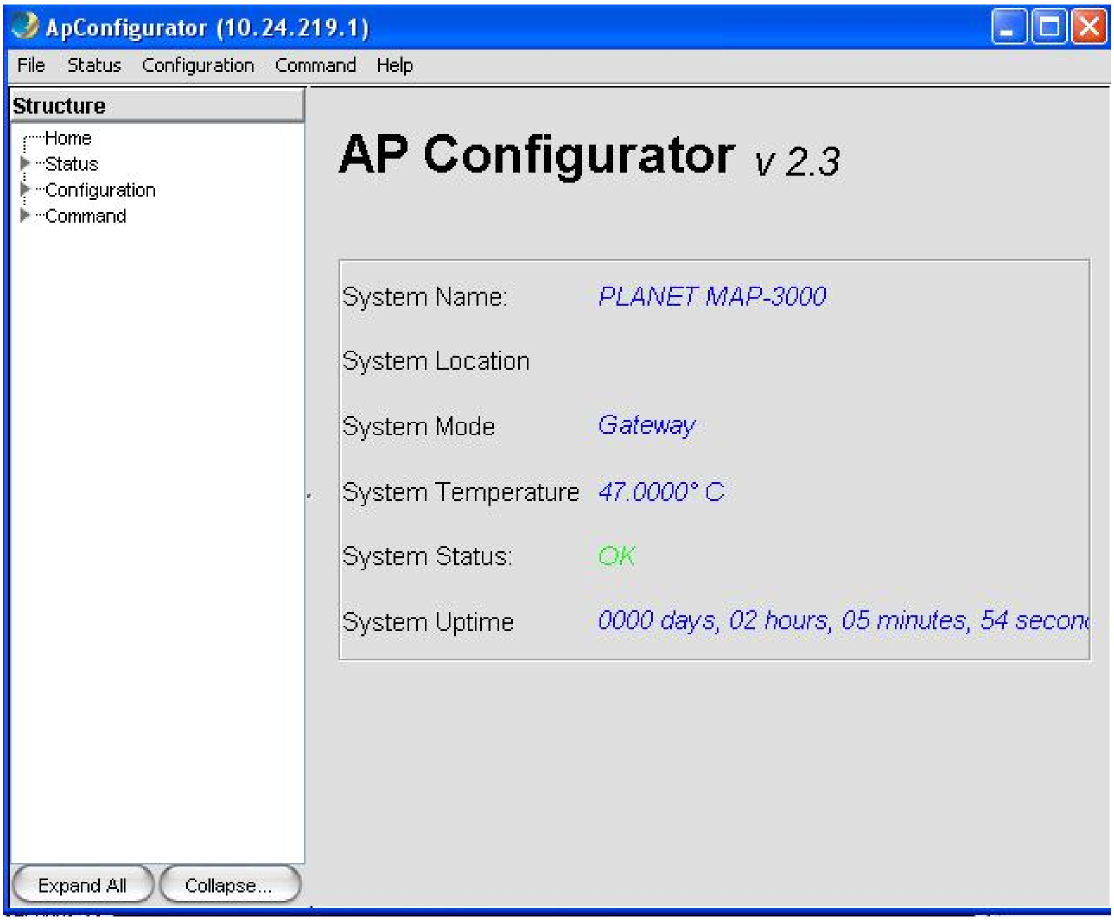
5 Configure the Mesh AP using AP Configurator

5.1 Overview of AP Configurator

One of the main features of the PLANET Mesh Network Management Tools is its ability to configure the Mesh AP remotely. In stead of the Web-Based Configuration page, user can use the application software that designed specifically for the configuration of the Mesh AP, namely the AP Configurator.

The AP Configurator utilizes the SNMP protocol to connect the user's terminal with the AP over the network. The AP Configurator supports all SNMP version 1, 2C and 3 over UDP. User may read and write the settings of the hardware through the SNMP agent running on the device.

The figure below illustrates the screenshot of the AP Configurator:



System Name: PLANET MAP-3000

System Location

System Mode Gateway

System Temperature 47.0000° C

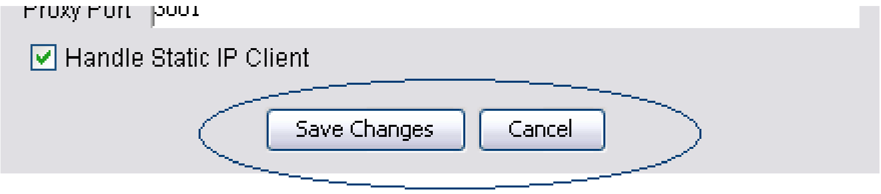
System Status: OK

System Uptime 0000 days, 02 hours, 05 minutes, 54 secon

5.2 How to use AP Configurator

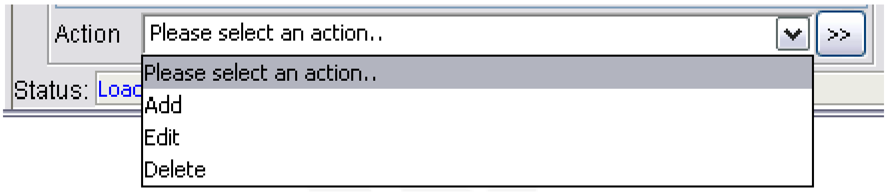
This section briefly explains how to configure the AP with the AP Configurator commonly. Before we proceed, let us have a quick view over the layout of the user interface. Thru the image at above, there is a tree at the left of the software. The tree lists all the configuration items in the AP. Click on the item that you wish to view or alter; the relative page will be loaded in the center frame. On the other hand, the menu bar on the top of the software can be used to open the configuration page as well.

There is a status bar at the bottom of the page, where it displays the status of the data loading and setting. In order to set the scalar values, perform the change, and click on the **Save Changes** button. The **Cancel** button is to close the configuration page.

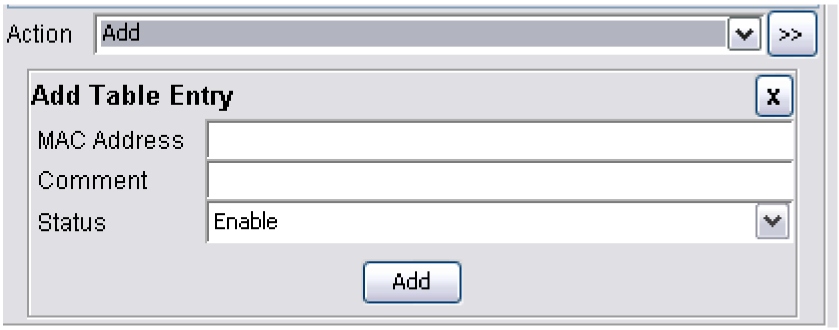


☑ Handle Static IP Client

In case to configure any table data, notice that there is a Status drop-down list at the bottom of every table, as shown:

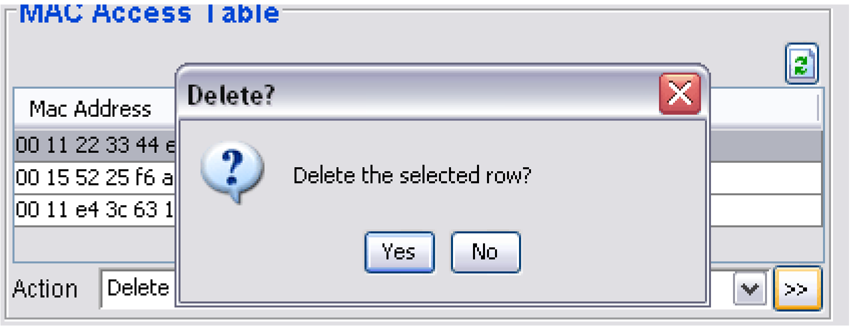


Select the type of action you would like to perform: add, edit or delete a table row. Then, click the “>>” button next to the drop-down list. For add and edit operation, an extra area will appear at the bottom of the drop down list, where it enable user to enter the table data. Hit the **Add** or **Edit** button to complete the operation. The area can be closed by selecting the “**X**” button at the top right corner.


Action: Add

Status: Enable

For delete action instead, select the table entry that wanted to be removed, click the “>>” button next to the drop-down list. A warning message would appear to prompt user for their confirmation to proceed with the operation. Hit **Yes** to proceed.



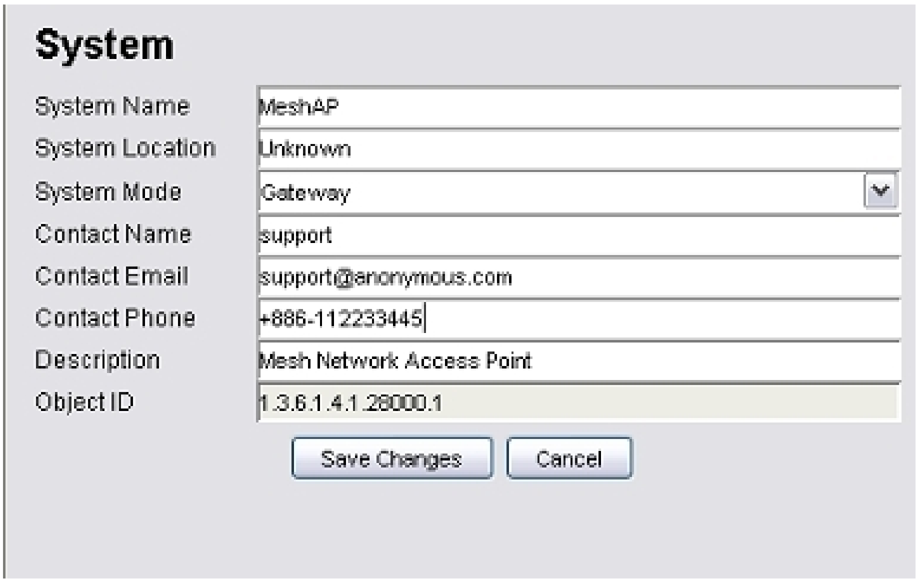
Delete the selected row?

The **Refresh** button at the top of every table is used to reload the table.

5.3 Configure the Mesh AP

At this section, we will look into every configuration pages of the Mesh AP one by one, and briefly describe the parameters in the pages.

5.3.1.1 System > System



System

System Name	MeshAP
System Location	Unknown
System Mode	Gateway
Contact Name	support
Contact Email	support@anonymous.com
Contact Phone	+886-112233445
Description	Mesh Network Access Point
Object ID	1.3.6.1.4.1.28000.1

The System page is the general settings page of the AP.

<u>Parameters:</u>

1) System Name
   - The generic name of the Mesh AP unit.
   - Data type: Display String

2) System Location
   - The generic physical location name of the Mesh AP Unit
   - Data type: Display String

3) System Mode
   - The operation mode of the Mesh AP unit
   - Options: Gateway, Relay, Client-relay, Layer 2 Gateway, Layer 2 Relay

Gateway	Layer 3 Gateway Mode. In a Mesh network Gateway mode is the path to the Internet for the whole Mesh network behind. WAN port is active and will be used for Internet Connection. Three types of Internet connection will be available, please refer

	to section 3.3.2 for more.
Relay	Layer 3 Relay Mode. Relay mode can help to route between mesh backhaul and local WiFi/LAN network. Also, a Relay mode Mesh AP can help to route the packets from other Relay node to the destination IP subnet or Gateway. WAN port is disabled at this mode. At the same time no WAN setting is required.
Client-Relay	Layer 3 Client-Relay Mode. At this mode, the Mesh node can only route between local WiFi/LAN network to mesh backhaul. It will not help to route packets from other Relay node. This mode can be used to reduce the unnecessary routing especially if this Mesh node is in the edge of the whole mesh topology.
Layer 2 Gateway	Layer 2 Gateway Mode. At this mode, the Mesh AP can be viewed as a bridge. This bridge can bridge between WAN, LAN, Mesh backhaul, and WiFi. As a Gateway, the WAN interface will turns into the public bridge port that connects to the existing Ethernet network. Be noted, only ONE Gateway is allowed in the same Mesh network.
Layer 2 Relay	Layer 2 Relay Mode. At this mode, the Mesh node act as a mesh relay that can bridge between WAN, LAN, Mesh backhaul and WiFi.

4) Contact Name

- The name of the contact person / network administrator
- Data type: Display String

5) Contact Email

- The E-mail address of the contact person / network administrator
- Data type: Display String

6) Contact Phone

- The phone number of the contact person / network administrator
- Data type: Display String

7) Description

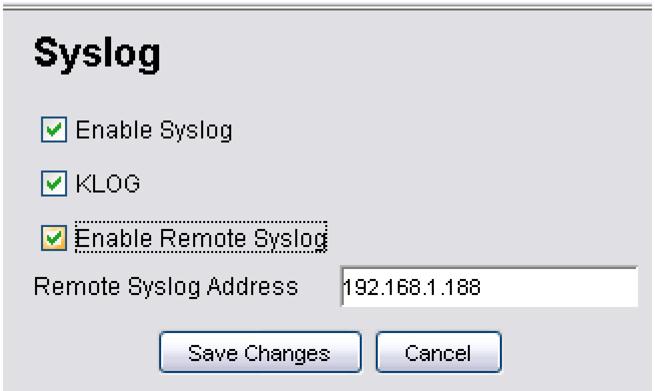
- A short description regarding the managed device (Mesh AP)
- Data type: Display String

8) Object ID

- The Object ID (OID) of the Mesh AP specified to support the SNMP service

- Read-only data

5.3.1.2 System > Syslog



Syslog

☑ Enable Syslog

☑ KLOG

☑ Enable Remote Syslog

Remote Syslog Address: 192.168.1.188

The Syslog is a system feature to send the system log messages to a remote server.

<u>Parameter</u>

1) Enable Syslog
   - A checkbox to enable or disable the syslog feature.

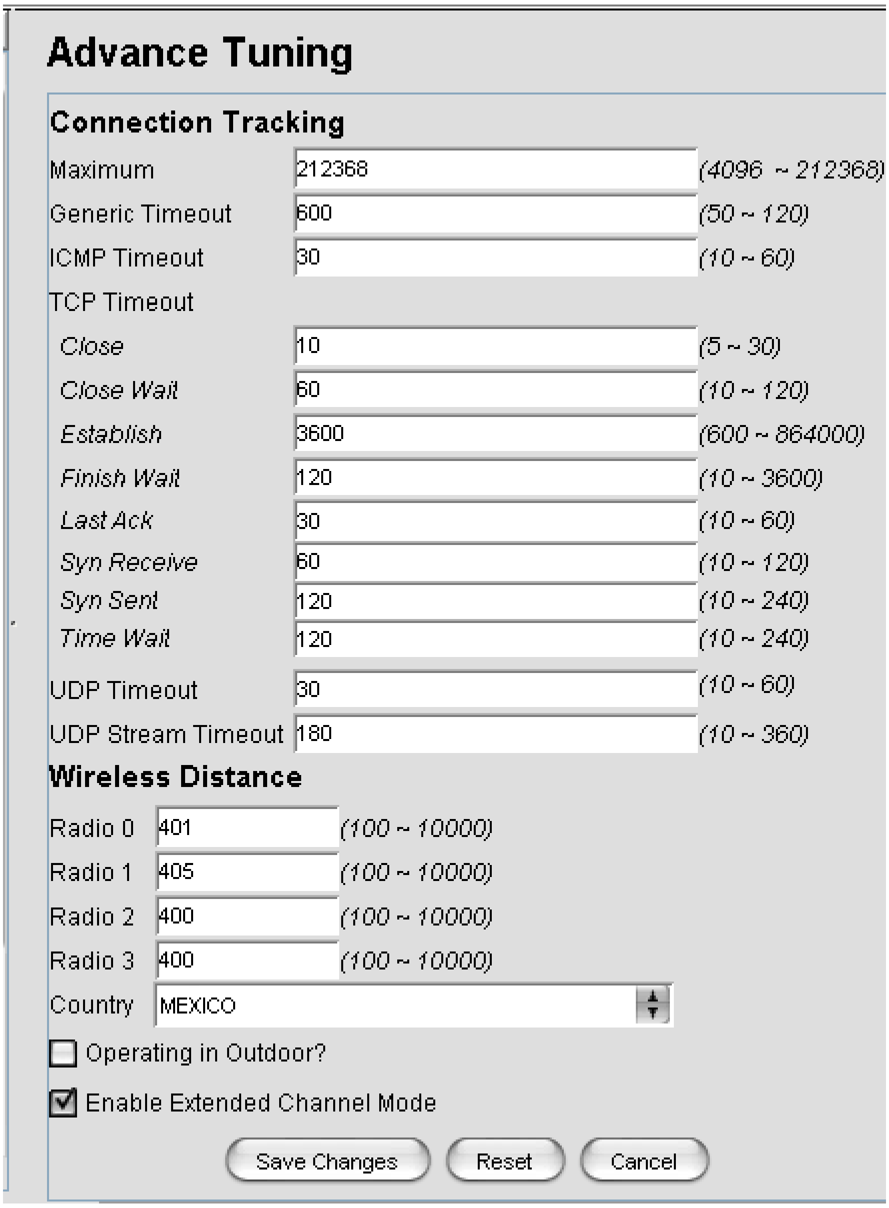
2) KLOG
   - A checkbox to enable or disable the Kernel Log service

3) Enable Remote Syslog
   a. A checkbox to enable or disable the remote syslog server service

4) Remote Syslog Address
   - The address of the remote syslog server, who will receive all the syslog message
   - Data type: DNS String

5.3.1.3 System > Advanced Tuning

The Advance Tuning panel is divided to two parts, the connection tracking parameters and the wireless distance. The Connection tracking portion determines the seconds of various timeout parameters, where as the latter define the estimate operating distance in meters, for the radio available in the device. Use the reset button to refill the value fields with the default values.



Advance Tuning

Connection Tracking

Maximum	212368	(4096 ~ 212368)
Generic Timeout	600	(50 ~ 120)
ICMP Timeout	30	(10 ~ 60)
TCP Timeout		
Close	10	(5 ~ 30)
Close Wait	60	(10 ~ 120)
Establish	3600	(600 ~ 864000)
Finish Wait	120	(10 ~ 3600)
Last Ack	30	(10 ~ 60)
Syn Receive	60	(10 ~ 120)
Syn Sent	120	(10 ~ 240)
Time Wait	120	(10 ~ 240)
UDP Timeout	30	(10 ~ 60)
UDP Stream Timeout	180	(10 ~ 360)

Wireless Distance

Radio 0	401	(100 ~ 10000)
Radio 1	405	(100 ~ 10000)
Radio 2	400	(100 ~ 10000)
Radio 3	400	(100 ~ 10000)
Country	MEXICO	

☐ Operating in Outdoor?

☑ Enable Extended Channel Mode

Parameters:

1) Maximum session
   - Maximum allowable IP connection tracking session.
   - Range: 4096 ~ 212368; Default: 10000 sessions
2) Generic Timeout
   - Timeout value in seconds (s) for generic connection track entry.
   - Range: 50 ~ 1200; Default: 600 seconds.
3) ICMP Timeout
   - Timeout value in seconds (s) for ICMP entry.
   - Range: 10 ~ 60; Default: 30 seconds.
4) TCP Close Timeout
   - Timeout value in seconds (s) for TCP close.
   - Range: 5 ~ 30; Default: 10 seconds.
5) TCP Close Wait Timeout

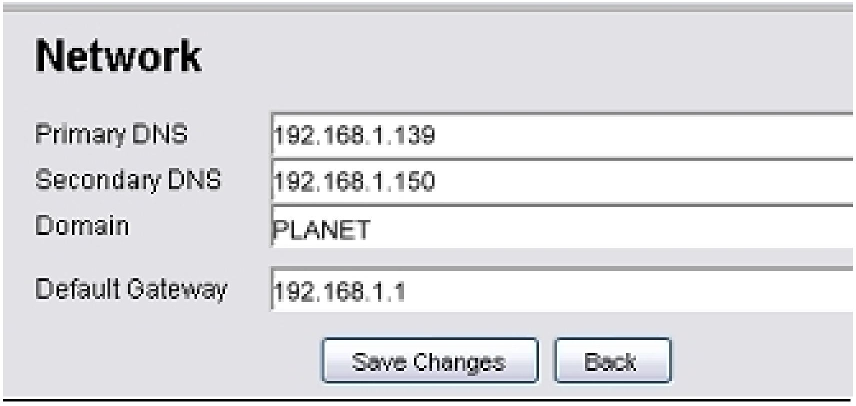
- Timeout value in seconds (s) for TCP close wait.
- Range: 10 ~ 120; Default: 60 seconds.

6) TCP Established Timeout
   - Timeout value in seconds (s) for established TCP.
   - Range: 600 ~ 864000; Default: 3600 seconds.
7) TCP Finished Wait Timeout
   - Timeout value in seconds (s) for TCP finished wait.
   - Range: 10 ~ 3600; Default: 120 seconds.
8) TCP Last ACK Timeout
   - Timeout value in seconds (s) for TCP last acknowledgement.
   - Range: 10 ~ 60; Default: 30 seconds.
9) TCP SYN Receive Timeout
   - Timeout value in seconds (s) for TCP SYN receive.
   - Range: 10 ~ 120; Default: 60 seconds.
10) TCP SYN Sent Timeout
    - Timeout value in seconds (s) for TCP SYN sent.
    - Range: 10 ~ 240; Default: 120 seconds.
11) TCP Time Wait Timeout
    - Timeout value in seconds (s) for TCP time wait.
    - Range: 10 ~ 240; Default: 120 seconds.
12) UDP Timeout
    - Timeout value in seconds (s) for UDP.
    - Range: 10 ~ 60; Default: 30 seconds.
13) UDP Stream Timeout
    - Timeout value in seconds (s) for UDP stream.
    - Range: 10 ~ 360; Default: 180 seconds.
14) Radio 1 distance
    - Specify the operating radius in meter (m) of radio 1.
    - Range: 100 ~ 10000; Default: 400 meters.
15) Radio 2 distance
    - Specify the operating radius in meter (m) of radio 2.
    - Range: 100 ~ 10000; Default: 400 meters.
16) Country
    - Select the operating country of the wireless interface.
17) Outdoor Mode
    - Enable or Disable the outdoor mode for the wireless interface.
    - Default: Enable.
18) External Channel Mode
    - Enable or Disable the external channel mode for the wireless interface.

- Default: Disable.

5.3.1.4 Network > Network

The network panel defines the DNS settings. This DNS service translates the domain name into IP Address form, which recognized by the Internet. If the primary server failed to perform the translation, the secondary server will take over the process.



Network

Primary DNS 192.168.1.139

Secondary DNS 192.168.1.150

Domain PLANET

Default Gateway 192.168.1.1

Parameters:

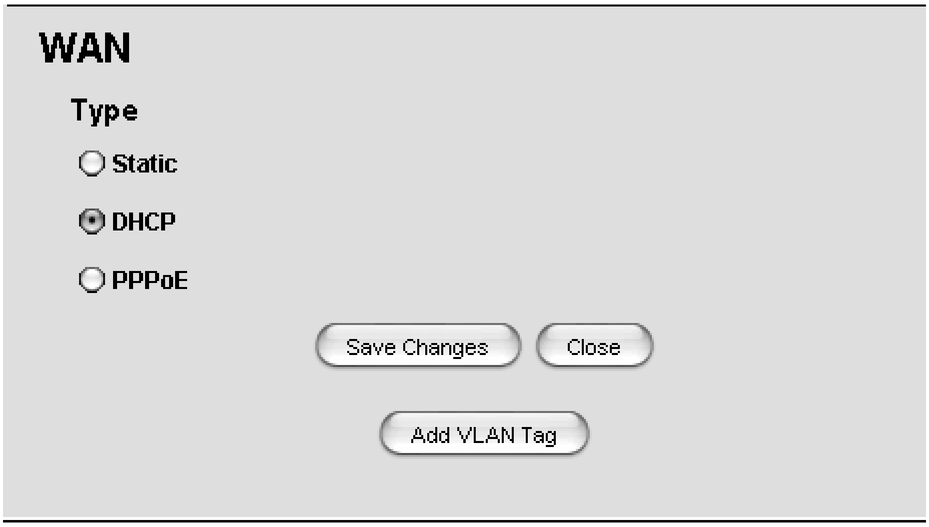
1) Primary DNS
- Define the Primary DNS Server IP Address.
- Data Type: IP Address

2) Secondary DNS
- Define the secondary DNS Server IP Address
- Data type: IP Address

3) Domain
- An optional domain name for the DNS client
- Data type: DNS String

4) Default Gateway
- The default gateway IP Address for the static IP Address
- Data type: IP Address

5.3.1.5 Network > WAN



WAN

Type

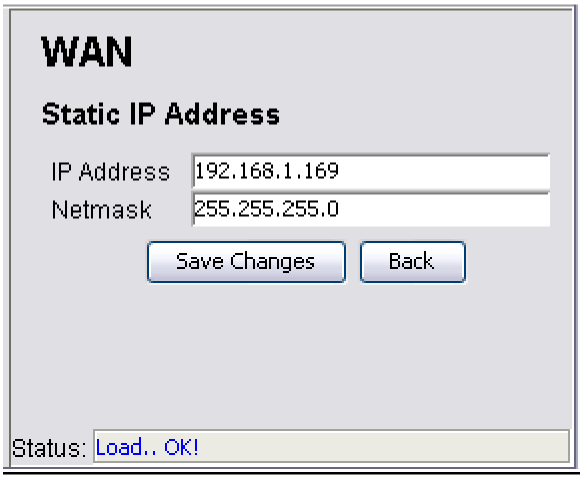
○ Static

● DHCP

○ PPPoE

Define the type of WAN interface to use. Three options are available: Static, DHCP, and PPPoE. If user wishes to change the type to dynamic, select the DHCP, then click the **Save Changes** button. If Static or PPPoE is selected instead, the **Configure** button will lead the user to the configuration page of the type.

- **Network > WAN > Static**



WAN

Static IP Address

IP Address 192.168.1.169

Netmask 255.255.255.0

Status: Load.. OK!

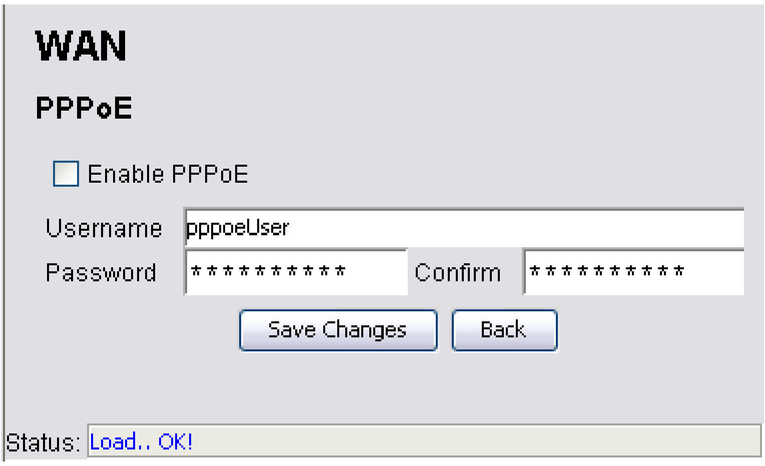
Enter the Static IP Address and its netmask, click the **Save Changes** button to activate the Static WAN interface type. Hit the **Back** to go back to the WAN Type configuration page.

Parameters:

1) IP Address
   - The static IP Address for the WAN interface
   - Data type: IP Address

2) Netmask
    - The netmask for the Static IP Address.
    - Data type: IP Address

- **Network > WAN > PPPoE**



WAN

PPPoE

□ Enable PPPoE

Username: pppoeUser

Password: ********** Confirm: **********

Status: Load.. OK!

Fill in the PPPoE’s username and password, then click the **Save Changes** button to activate the PPPoE WAN interface type. Hit the **Back** button to back to the WAN Type configuration page.

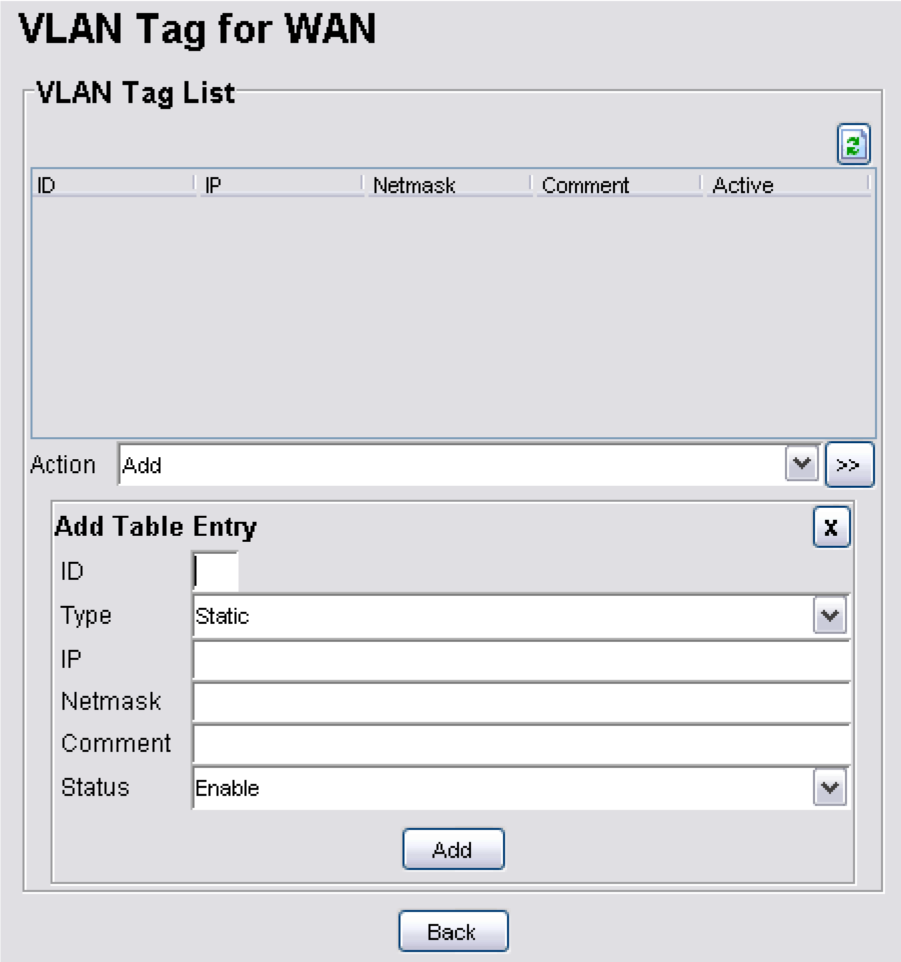
Parameters:

1) Enable PPPoE
    - A checkbox to enable or disable the PPPoE service.

2) Username
    - The username of the PPPoE client
    - Data type: Display String

3) Password, Confirm
    - The password corresponding to the username of the PPPoE client
    - Must key in the same input at the Confirm field to avoid mistakes
    - Data type: Display String

- **Network > WAN > Add VLAN Tag**



VLAN Tag for WAN

VLAN Tag List

ID	IP	Netmask	Comment	Active

Action: Add

Add Table Entry

ID:

Type: Static

IP:

Netmask:

Comment:

Status: Enable

Note that there is an **Add VLAN Tag** button at the WAN page. Press the button would open the VLAN Tag page, where user may define the VLAN ID for a desired WAN interface.

Note

1. If your Ethernet network that connect to WAN port supports VLAN tagging and you plan to make the Mesh Network route for different purpose, you can use the "Add VLAN Tag" button to create different VLAN for WAN interface.
2. Only the **default WAN** is **un-tagged**. Any other newly inserted WAN interface will be tagged follow the ID setting that range from 1 to 4095. Maximum is 15 virtual WAN interfaces are allowed.

Parameters (VLAN Tag List columns)

1) ID
   - The VLAN-ID
   - Data type: Integer, in between 1 and 4096

2) Type
   - The type of the WAN-VLAN defined.

- Available option: Static and DHCP

3) IP
    - The IP Address of the interface.
    - This field is disabled if the Type chosen is DHCP
    - Data type: IP Address

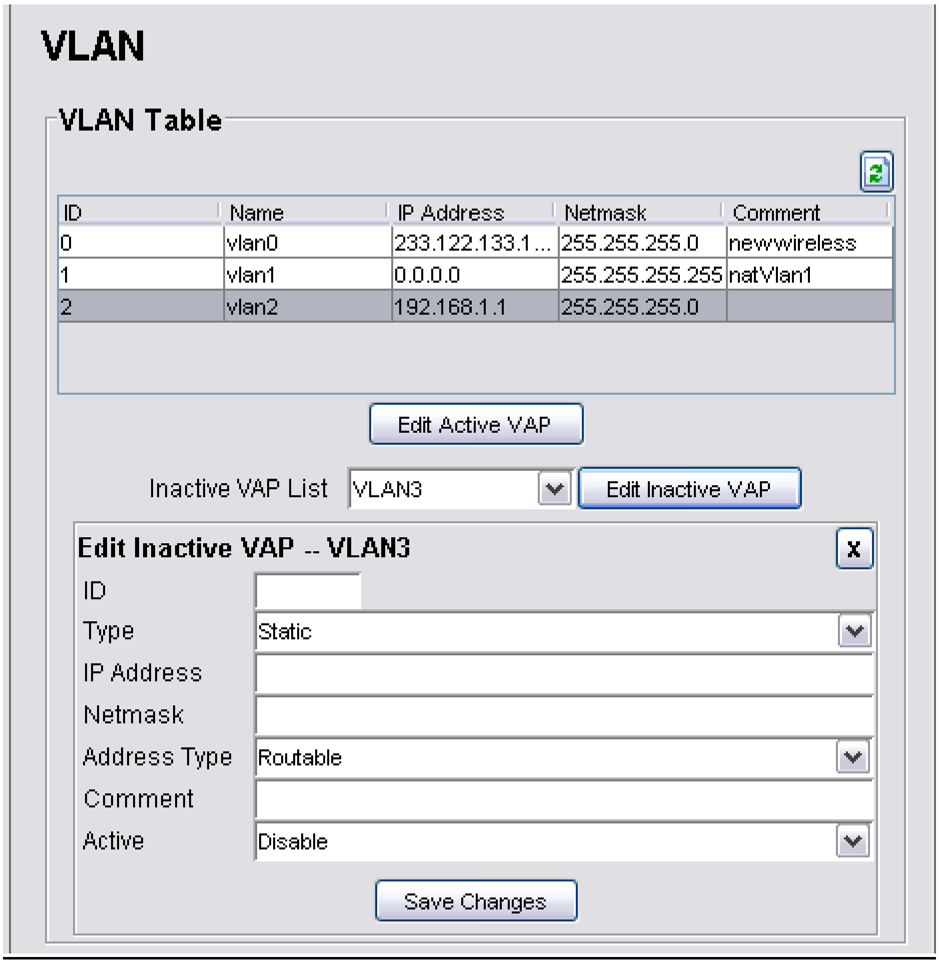
4) Subnet
    - The corresponding subnet for the IP Address of the interface.
    - This field is disabled if the Type chosen is DHCP
    - Data type: IP Address

5) Comment
    - Optional comment regarding the table entry
    - Data type: Display String

6) Status
    - Enable or disable the table entry.
    - Available option: Enable and Disable

Hit the **Back** button to go back to the WAN-Type page.

5.3.1.6 Network > VLAN



VLAN

VLAN Table

ID	Name	IP Address	Netmask	Comment
0	vlan0	233.122.133.1…	255.255.255.0	newwireless
1	vlan1	0.0.0.0	255.255.255.255	natVlan1
2	vlan2	192.168.1.1	255.255.255.0	

Edit Active VAP

Inactive VAP List: VLAN3 — Edit Inactive VAP

Edit Inactive VAP -- VLAN3

ID	
Type	Static
IP Address	
Netmask	
Address Type	Routable
Comment	
Active	Disable

Save Changes

The page is displaying the VLAN Table which is showing the activated VAP of the Mesh AP. There are total of 16 VLANs available in the device. In order to activate an inactive VAP, choose an entry from the Inactive VAP List, then click the **Edit Inactive VAP** button. Then the Edit Inactive VAP – VLANx panel would appear. Similarly, to edit or disable an active VAP, user can select the entry from the table, and hit the **Edit Active VAP**. Fill in the following parameters:

1) ID
   - The ID for the VLAN interface.
   - The value is ranged between 1 to 4095, where 0 is reserved for VLAN0

2) Type
   - The type of the VLAN
   - The available options are static and dynamic

3) IP Address
    - The IP Address of the selected VLAN interface

4) Netmask
    - The Netmask for the IP Address

5) Address Type
    - The type of the IP Address, either NAT or Routable

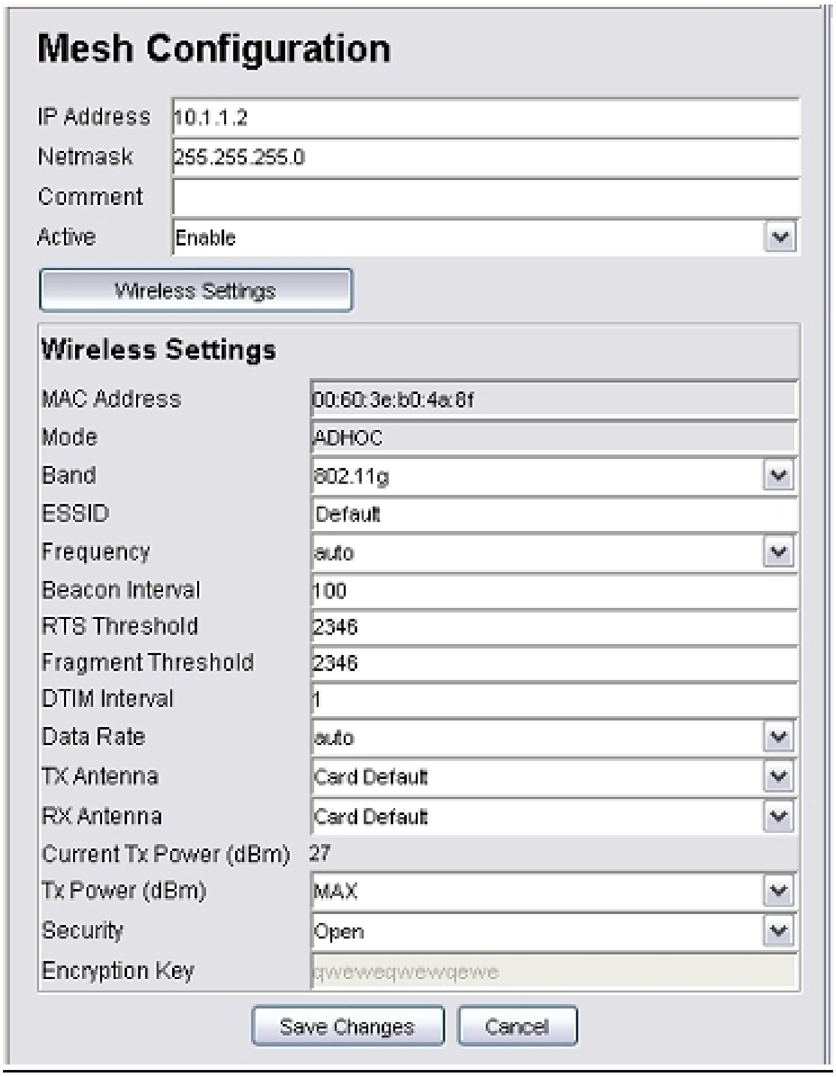
6) Comment
    - An optional comment regarding the table entry

7) Active
    - The status of the VAP
    - Set to Active to enable an inactive VAP; set to Inactive to disable an active VAP.

Finally click the **Save Changes** button to commit the changes.

⚠ ***Note***	1. ONLY VLAN 0, the default VLAN, is un-tagged packets. For VLAN 1 to VLAN 15, it will be tagged packets at LAN interface after it is enabled. And for Wireless interface, different SSID are required for different VLAN. 2. The connected LAN device should support VLAN tagging if you plan to connect wired device for different VLAN.

5.3.1.7 Network > Mesh



Mesh Configuration

IP Address	10.1.1.2
Netmask	255.255.255.0
Comment	
Active	Enable

Wireless Settings

MAC Address	00:60:3e:b0:4a:8f
Mode	ADHOC
Band	802.11g
ESSID	Default
Frequency	auto
Beacon Interval	100
RTS Threshold	2346
Fragment Threshold	2346
DTIM Interval	1
Data Rate	auto
TX Antenna	Card Default
RX Antenna	Card Default
Current Tx Power (dBm)	27
Tx Power (dBm)	MAX
Security	Open
Encryption Key	qweweqwewqewe

The Mesh configuration page read the data from the wireless interface, ath0. Select the **Wireless Settings** button to view or edit the corresponding data.

Parameters (Mesh Configuration)

1) IP Address
   - IP Address for the Mesh interface
   - Data type: IP Address

2) Netmask
   - Netmask for the IP Address of the Mesh interface
   - Data type: IP Address

3) Comment

- An optional comment regarding the Mesh interface
- Data type: Display String

4) Active
   - The status of the Mesh interface, either active or inactive.

Parameters (Wireless Settings)

1) MAC Address
   - The Mac Address of the Mesh interface
   - This is a read-only parameter

2) Mode
   - Define the mode of the Mesh interface
   - In this case, the mode is fixed to AD-HOC

3) Band
   - The band to use
   - Three options available: 802.11a, 802.11b, and 802.11g

4) ESSID
   - The identifying name of a wireless access point's network
   - Data type: Display String

5) Frequency
   - The operating frequency of the ath0 wireless network interface in Mega Hertz.

6) Beacon Interval
   - The beacon interval in milliseconds
   - Data type: Integer, in between 20 and 1000
   - Default value is 100

7) RTS Threshold
   - The RTS Threshold value
   - Data type: Integer, in between 256 and 2346
   - Default value is 2346

8) Fragment Threshold
   - The Fragment Threshold value

- Data type: Integer, even number only, in between 1500 and 2346
- Default value is 2346

9) DTIM Interval
   - Data type: Integer, in between 1 and 256
   - Default value is 1

10) Data Rate
    - Select the data rate of the interface from the list
    - Available selection: Auto, 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps

11) TX Antenna
    - The properties of the transmission antenna
    - Available selection: Diversity, Port1, Port2 and Card Default

12) RX Antenna
    - The properties of the reception antenna
    - Available selection: Diversity, Port1, Port2 and Card Default

13) Current Tx Power (dBm)
    - This is a read-only field indicating the current transmission power used by the mesh interface.
    - The value is in the unit of dBm

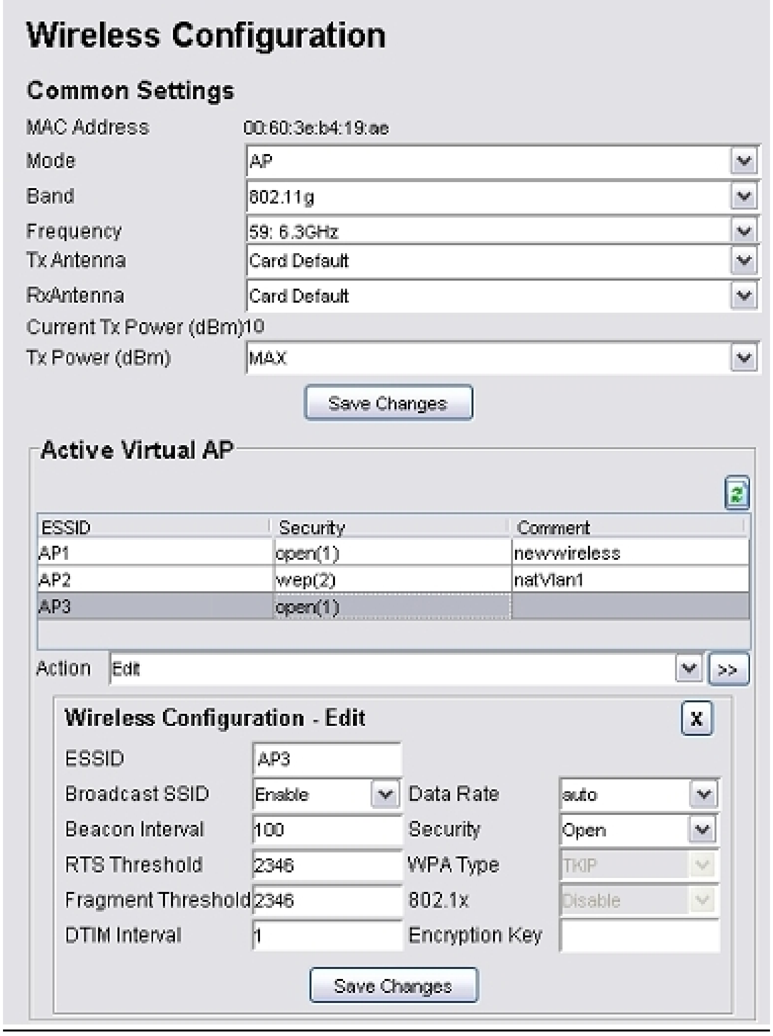
14) Tx Power (dBm)
    - The transmission power field, where user can alter the level of power through the selection available.
    - The default value for this field is Max, which will use the maximum power level of the wireless interface.

15) Security
    - The security type to be used by the wireless network, wither open, WEP, or AES

16) Encryption Key
    - The encryption key used in corresponding to the security type used.
    - Data type: Octet String

5.3.1.8 Network > Wireless Configuration

The upper portion of the Wireless Configuration page is displaying the common settings of all the wireless interfaces. The parameters here will be applied to all the VAP. The table in the page is showing the list of virtual APs. User can only edit the information in the table.



Wireless Configuration

Common Settings

MAC Address 00:60:3e:b4:19:ae
Mode AP
Band 802.11g
Frequency 59: 6.3GHz
Tx Antenna Card Default
RxAntenna Card Default
Current Tx Power (dBm)10
Tx Power (dBm) MAX

Active Virtual AP

ESSID	Security	Comment
AP1	open(1)	newwireless
AP2	wep(2)	natVlan1
AP3	open(1)	

Action Edit

Wireless Configuration - Edit

ESSID	AP3		
Broadcast SSID	Enable	Data Rate	auto
Beacon Interval	100	Security	Open
RTS Threshold	2346	WPA Type	TKIP
Fragment Threshold	2346	802.1x	Disable
DTIM Interval	1	Encryption Key	

Parameters (Common Settings)

1) MAC Address
   - The Mac Address of the Wireless interface
   - This is a read-only parameter

2) Mode
   - The Mode is fixed to AP

3) Band
   - The band to use

- Three options available: 802.11a, 802.11b, and 802.11g

4) Frequency
   - The operating frequency of the ath1 wireless network interface in Mega Hertz

5) TX Antenna
   - The properties of the transmission antenna
   - Available selection: Diversity, Port1, Port2 and Card Default

6) RX Antenna
   - The properties of the reception antenna
   - Available selection: Diversity, Port1, Port2 and Card Default

7) Current Tx Power (dBm)
   - This read-only field indicating the current transmission power level used by the wireless interface.
   - The value is in the unit of dBm

8) Tx Power (dBm)
   - The transmission power level of the wireless interface
   - The default value is Max, where the device will tune the transmission power to the maximum level of the wireless interface.

Click the **Save Changes** button to commit the common configurations.

Parameters (Virtual AP list)

1) ESSID
   - The Enhanced Service Set Identifier of the wireless network
   - Data type: Display String

2) Broadcast SSID
   - Enable or disable the SSID to be broadcasted.

3) Beacon Interval
   - The beacon interval in milliseconds
   - Data type: Integer, in between 20 and 1000
   - Default value is 100

4) RTS Threshold
    - The RTS Threshold value
    - Data type: Integer, in between 256 and 2346
    - Default value is 2346

5) Fragment Threshold
    - The Fragment Threshold value
    - Data type: Integer, even number only, in between 1500 and 2346
    - Default value is 2346

6) DTIM Interval
    - DTIM Interval
    - Data type: Integer, in between 1 and 256
    - Default value is 1

7) Data Rate
    - Select the data rate of the interface from the list
    - Available selection: Auto, 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps

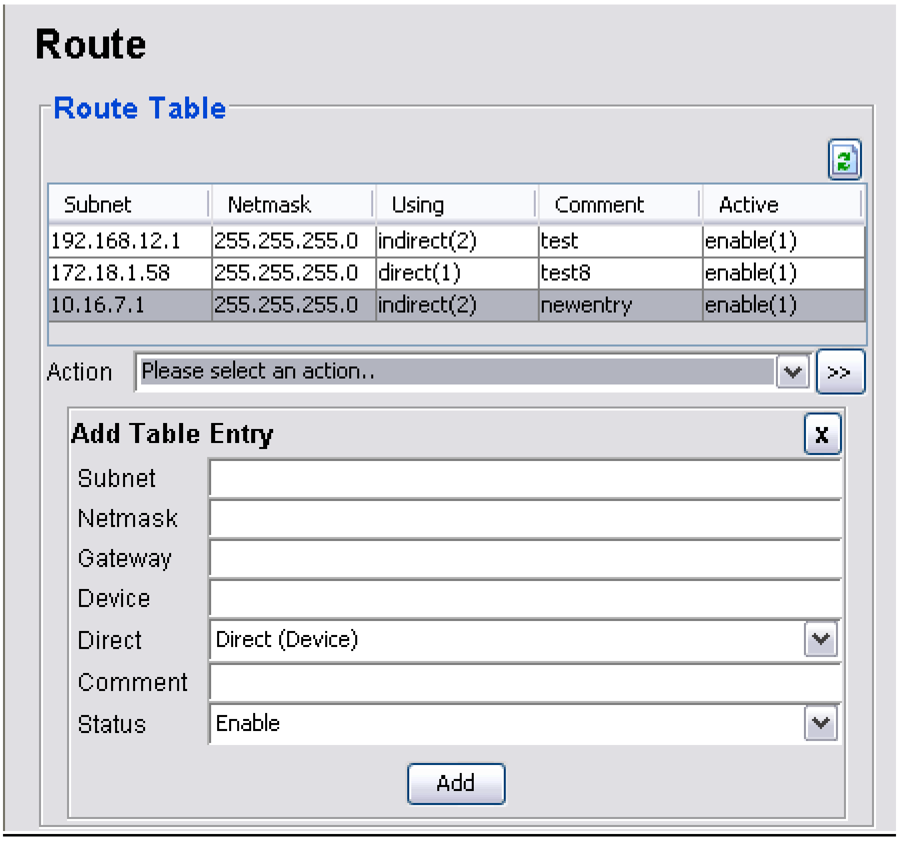
8) Security
    - The security type, can be either Open, WEP, WPA1, WPA2, and WPA1&2

9) WPA-Type
    - The type of the WPA security mode
    - Available options: TKIP and AES
    - This field is only writable if the security type WPA is selected

10) 802.1x
    - Enable or disable the use of Radius Server as authenticator
    - This field is only enabled if WEP or WPA is selected

11) Encryption Key
    - The encryption key depends on the type of security mode using
    - This field is only enabled if WEP or WPA is selected

5.3.1.9 Network > Route



Route

Route Table

Subnet	Netmask	Using	Comment	Active
192.168.12.1	255.255.255.0	indirect(2)	test	enable(1)
172.18.1.58	255.255.255.0	direct(1)	test8	enable(1)
10.16.7.1	255.255.255.0	indirect(2)	newentry	enable(1)

Action: Please select an action.. >>

Add Table Entry

Subnet	
Netmask	
Gateway	
Device	
Direct	Direct (Device)
Comment	
Status	Enable

The route table is a network map that notifies the node about the way to deliver the packets to its addressee. This configuration page presents the routing table of the Mesh AP.

Parameters:

1) Subnet
   - The subnet address of the route
   - Data type: IP Address

2) Netmask
   - The netmask corresponding to the subnet address
   - Data type: IP Address

3) Gateway
   - The gateway IP Address for this route entry
   - Data type: IP Address

4) Device
   - Specifies the route devices for this route entry
   - Data type: Octet String

5) Direct

- Select the type of routing, either direct or indirect.
- Direct type using device, whereas indirect is using the two hope gateway

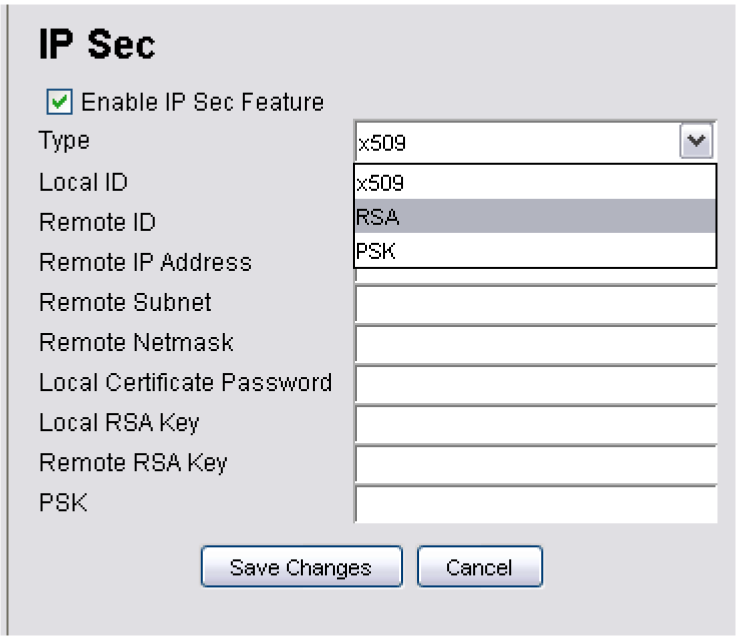
6) Comment

- An optional comment regarding the route table entry
- Data type: Display String

7) Status

- Specify the status of the route entry, enable or disable.

5.3.1.10 Network > IP Sec



IP Sec

☑ Enable IP Sec Feature

Type: x509

Local ID

Remote ID

Remote IP Address

Remote Subnet

Remote Netmask

Local Certificate Password

Local RSA Key

Remote RSA Key

PSK

The IP Sec configuration page enable user to alter the setting of the IP Security Protocol. With IPSec, a security “tunnel” is created between the source and destination point, allow the packet to be sent through the “tunnel”. In this page, user can define the characteristics, including the certificate key and RSA key, of the tunnel.

<u>Parameters:</u>

1) Enable IP Sec

- A checkbox to enable or disable the IPSec service.

2) Type

- Select the type of the IPSec protocol.
- Available selection:
    - x509
    - RSA
    - PSK

3) Local ID
    - The identifier of the local host.
    - Data type: Octet String
4) Remote ID
    - The identifier of the remote host at the other end
    - Data type: Octet String

5) Remote IP Address
    - The IP Address of the remote host.
    - Data type: IP Address

6) Remote Subnet, Remote Netmask
    - The Subnet where the remote host is located at, with its correspond netmask
    - Data type: IP Address

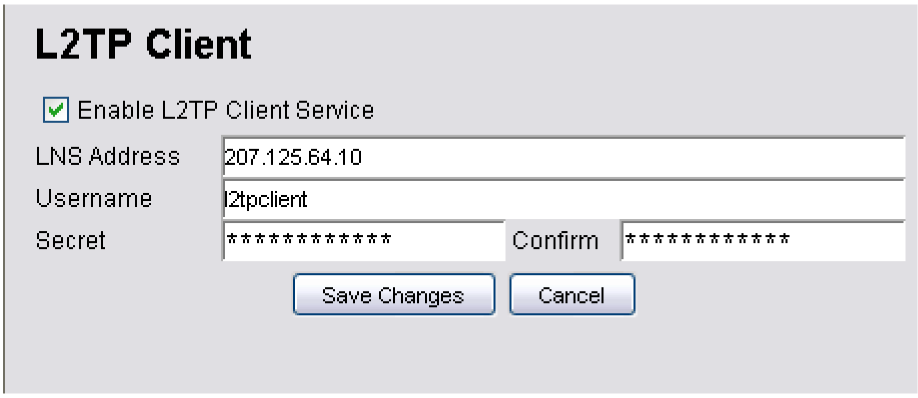
7) Local Certificate Password
    - The x.509 certificate pem passphrase, used when IPSec type x509 is selected
    - Data type: Octet String

8) Local RSA Key
    - The RSA Key of the local host, used when IPSec type RSA is selected
    - Data type: Octet String

9) Remote RSA Key
    - The RSA Key of the remote host, used when IPSec type RSA is selected
    - Data type: Octet String

10) PSK
    - The PSK Key, used when IP Sec type PSK is selected
    - Data type: Octet String

5.3.1.11 Network > L2TP Client



L2TP Client

☑ Enable L2TP Client Service

LNS Address: 207.125.64.10

Username: l2tpclient

Secret: ************* Confirm: *************

The L2TP (Layer 2 Tunneling Protocol) is a tunneling protocol that used to support the virtual private network. Admin can create a L2TP client at this panel for the network traffic tunneling purpose.

<u>Parameters</u>

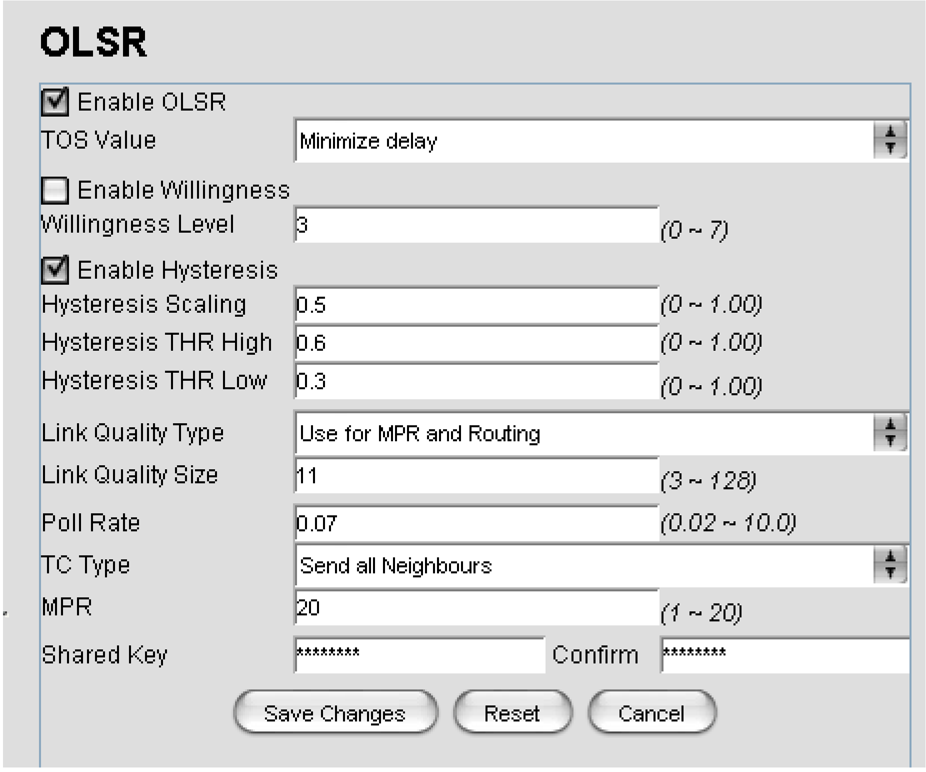
1) Enable L2TP Client Service
   - A checkbox to enable or disable the L2TP feature

2) LNS Address
   - The L2TP Network Server address.
   - Data type: DNS String

3) Username
   - The username for the L2TP client
   - Data type: Display String

4) Password
   - The correspond password for the username above
   - Data type: Display String

5.3.1.12 Network > OLSR



OLSR

☑ Enable OLSR		
TOS Value	Minimize delay	
☐ Enable Willingness		
Willingness Level	3	(0 ~ 7)
☑ Enable Hysteresis		
Hysteresis Scaling	0.5	(0 ~ 1.00)
Hysteresis THR High	0.6	(0 ~ 1.00)
Hysteresis THR Low	0.3	(0 ~ 1.00)
Link Quality Type	Use for MPR and Routing	
Link Quality Size	11	(3 ~ 128)
Poll Rate	0.07	(0.02 ~ 10.0)
TC Type	Send all Neighbours	
MPR	20	(1 ~ 20)
Shared Key	********	Confirm ********

The OLSR configuration page defines the Optimized Link State Routing protocol of the Mesh AP. It is a routing protocol for the Layer 3 mesh backhaul connections.

<u>Parameters</u>

1) Enable OLSR
   - A checkbox to enable the OLSR service

2) TOS Value
   - This field define the type of service value that should be set in the OLSR control traffic packet IP headers
   - Data type: Integer

3) Enable Willingness
   - A checkbox to enable the willingness of the Mesh AP.
   - Willingness of an AP is defined as the readiness of a node to carry and forward traffic for other nodes.

4) Willingness Level
   - The level of the willingness.
   - Data type: Integer (0-7)

5) Enable Hysteresis
   - A checkbox to enable the hysteresis of the Mesh AP
   - Link hysteresis determines the criteria at which a link to a neighbour is accepted or rejected. Hysteresis adds more robustness to the link sensing, but delays the neighbour registration.

6) Hysteresis Scaling
   - The level scale of the hysteresis
   - Data type: Float (0.0 ~ 1.0)

7) Hysteresis THR High
   - The upper limit (threshold high) of the hysteresis
   - Data type: Float (0.0 ~ 1.0)

8) Hysteresis THR Low
   - The lower limit (threshold low) of the hysteresis
   - Data type: Float (0.0 ~ 1.0)

9) Link Quality Type
   - The type of link quality
   - Available options:
     - Disable
     - Use for MPR selection
     - Use for MPR selection and Routing

10) Link Quality Size
    - The Link quality window size
    - Data type: Integer, default size is 10

11) Poll Rate
    - The polling rate, where the value is in the interval of 0 and 1
    - Data type: Float

12) TC Rate
    - The TC redundancy specifies the level of neighbour information should be sent in a TC message.
    - Available options:

  - Send only MPR Selectors
  - Send only MPR Selectors and MPRs
  - Send all neighbours

13) MPR

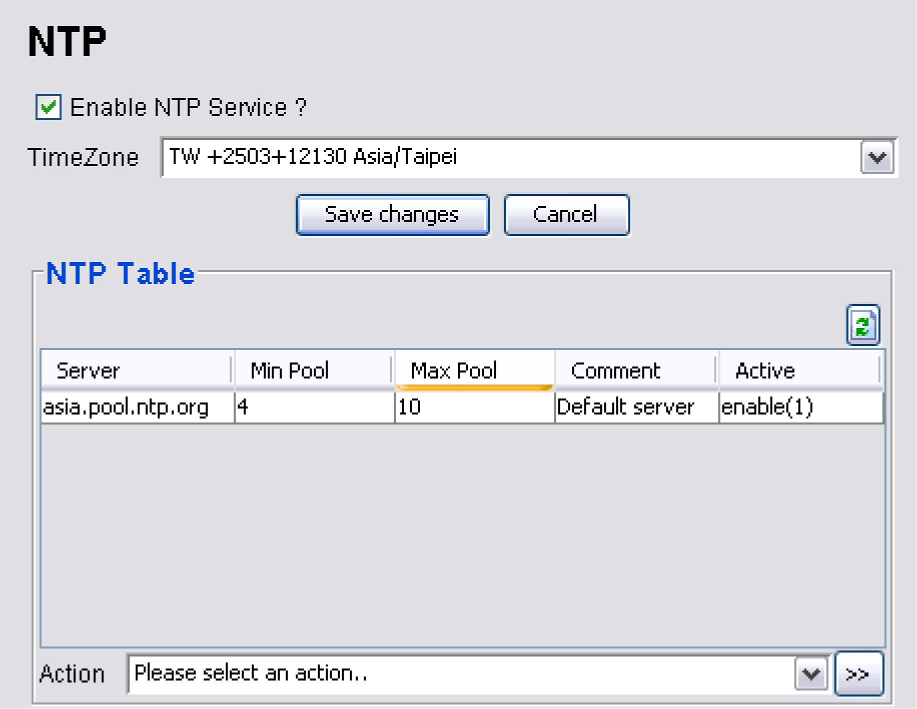
- This field specifies how many MPRs a node should try select to reach every 2hop neighbour
- Data type: Integer, default value is 1

14) Shared Key

- The secret shared key.
- User must re-enter the same password at the Confirm field to set this field
- Data type: Display String

Note Unless you are familiar with the setting, otherwise we would suggest to keep the value unchanged, or press Reset to set back to default. These settings should fit for the most application.

5.3.1.13 Services > NTP



NTP

☑ Enable NTP Service ?

TimeZone: TW +2503+12130 Asia/Taipei

Server	Min Pool	Max Pool	Comment	Active
asia.pool.ntp.org	4	10	Default server	enable(1)

Action: Please select an action..

The NTP service implements the Network Time Protocol to the Mesh APs to synchronize the system time to some time reference. The NTP Table in this page lists the NTP server that is used by the device.

Parameters

1) Enable NTP Service
    - A checkbox to enable the NTP service of the system

2) Time Zone
    - A list of time zones is available in the drop down list. Select the appropriate one to synchronize.

Parameters (NTP Table columns)

1) Server
    - The NTP server host name
    - Data type: DNS String

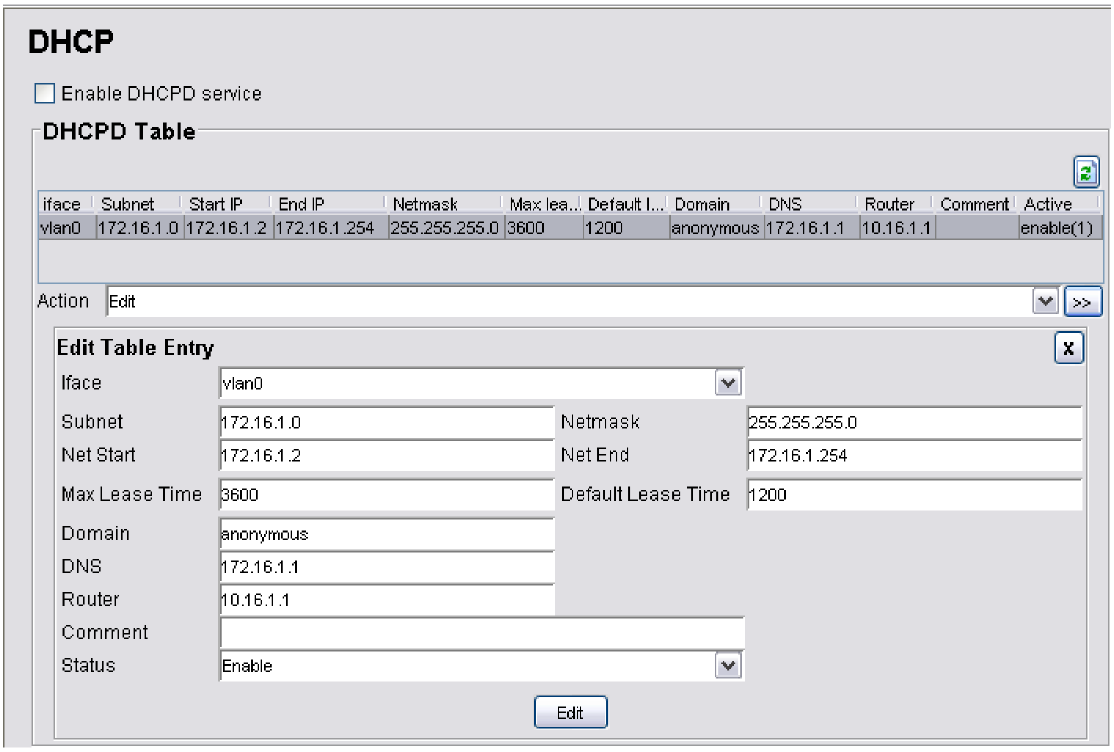
2) Min Pool
    - The minimum pool time of the server, in seconds
    - Data type: Integer, default value is 4

3) Max Pool
    - The maximum pool time of the server, in seconds
    - Data type: Integer, default value is 10

4) Comment
    - An optional comment regarding the NTP Table entry
    - Data type: Display String

5) Active
    - The status of the NTP Table entry, either active or inactive

5.3.1.14 Services > DHCP



DHCP

□ Enable DHCPD service

DHCPD Table

iface	Subnet	Start IP	End IP	Netmask	Max lea...	Default l...	Domain	DNS	Router	Comment	Active
vlan0	172.16.1.0	172.16.1.2	172.16.1.254	255.255.255.0	3600	1200	anonymous	172.16.1.1	10.16.1.1		enable(1)

Action: Edit

Edit Table Entry

Iface	vlan0		
Subnet	172.16.1.0	Netmask	255.255.255.0
Net Start	172.16.1.2	Net End	172.16.1.254
Max Lease Time	3600	Default Lease Time	1200
Domain	anonymous		
DNS	172.16.1.1		
Router	10.16.1.1		
Comment			
Status	Enable		

The DHCP service offers the Mesh AP a feature to assign dynamic IP Address to all the clients. The DHCPD Table in this configuration page lists the dynamic IP assignments in the device.

Parameters (DHCPD Table columns)

1) Iface
   - The name of the active interface in the Mesh AP unit.
   - Data type: Octet String

2) Subnet
   - The subnet address
   - Data type: IP Address

3) Netmask
   - The netmask corresponding to the subnet of the table entry
   - Data type: IP Address

4) Net Start
   - The starting IP Address in the subnet for the assignment.
   - Data type: IP Address

5) Net End
   - The last IP Address in the subnet for the assignment
   - Data type: IP Address

6) Max Lease Time
   - The maximum duration for the client to retain its current IP Address
   - Data type: Integer, in the range of 600 to 864000 seconds

7) Default Lease Time
   - The lease time defined for the client to retain its current IP Address. Once the time is up, the IP Address will be released.
   - Data type: Integer, in the range of 600 to 864000 seconds

8) Domain
   - The domain name for the DHCP Server
   - Data type: DNS String

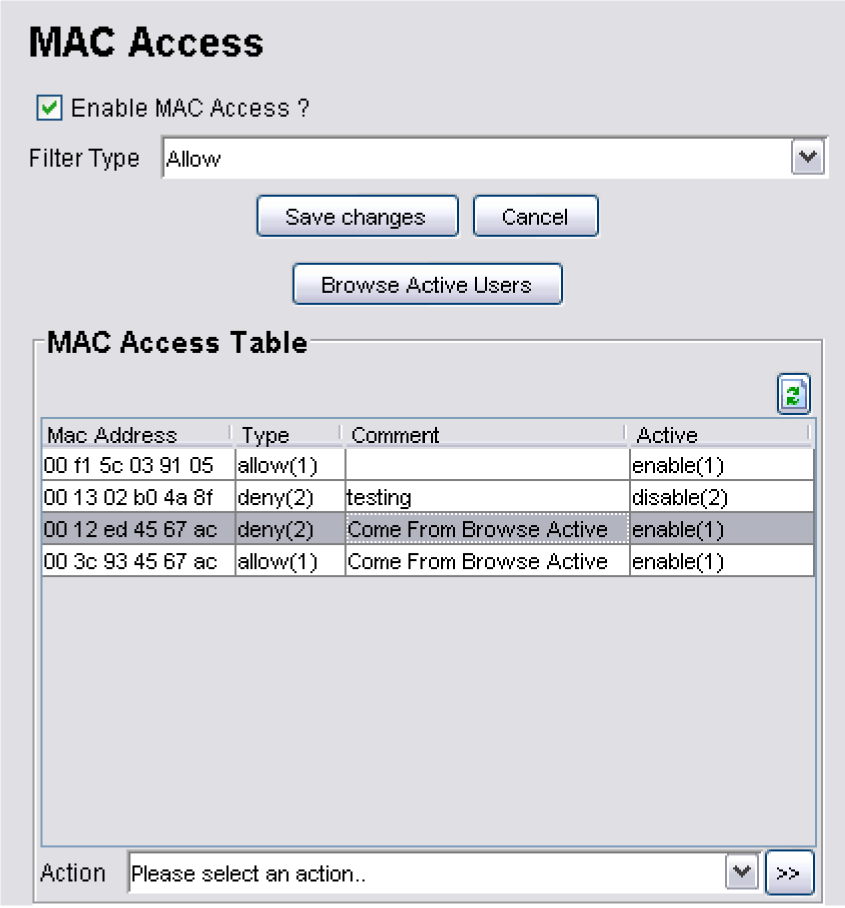
9) DNS
   - The IP Address of the DNS server of the subnet
   - Data type: IP Address

10) Router
   - The router IP Address of the subnet
   - Data type: IP Address

11) Comment
   - An optional comment for the particular table entry
   - Data type: Display String

12) Status
   - The status of that particular table entry, either active or inactive

5.3.1.15 Services > MAC Access



MAC Access

☑ Enable MAC Access ?

Filter Type: Allow

MAC Access Table

Mac Address	Type	Comment	Active
00 f1 5c 03 91 05	allow(1)		enable(1)
00 13 02 b0 4a 8f	deny(2)	testing	disable(2)
00 12 ed 45 67 ac	deny(2)	Come From Browse Active	enable(1)
00 3c 93 45 67 ac	allow(1)	Come From Browse Active	enable(1)

Action: Please select an action..

The Mac Access feature of the Mesh AP provides a filtering method to limit the accessing of the client. User can set the Mac Access Table to deny or inversely, allow the client that defined with their Mac Address to attach to the network.

Parameters:

1) Enable MAC Access

- A checkbox to enable or disable the MAC Access feature

2) Filter Type

- Define the filter type of the user not listed in the MAC Access Table, either to allow or deny the client entries to access the network.

Parameters (MAC Access Table)

1) Mac Address

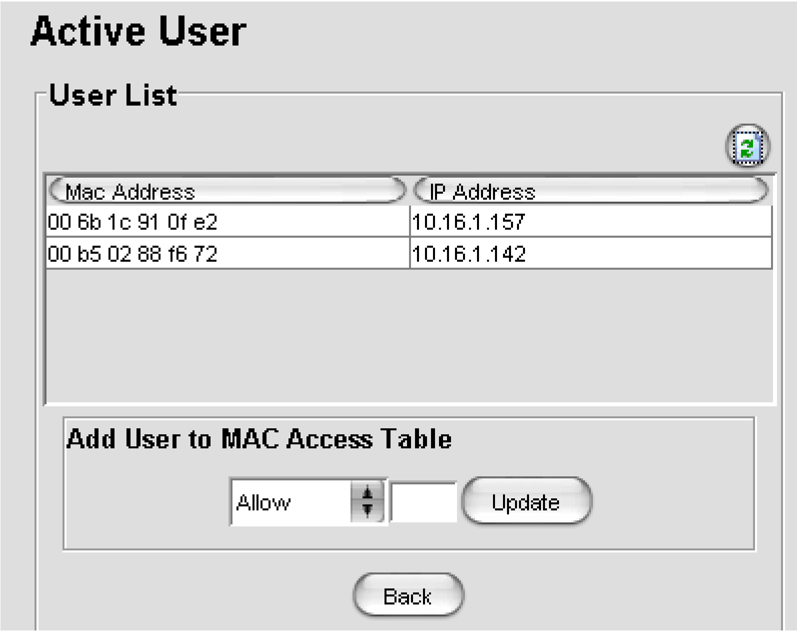
- The Mac Address of the client to be filtered.
- Data type: Mac Address

2) Type
   - Define the type of control for the corresponding Mac Address, either Allow or Deny

3) Comment
   - An optional comment regarding the client
   - Data type: Display String

4) Active
   - The status of the table entry, either active or inactive

The **Browse Active Users** button opens a list that shows every active user associating to the network. From this table, the administrator may add the desired user into the Mac Access Table, by using the **Update** button. Choose the type of accessing from the drop down list.



Active User

User List

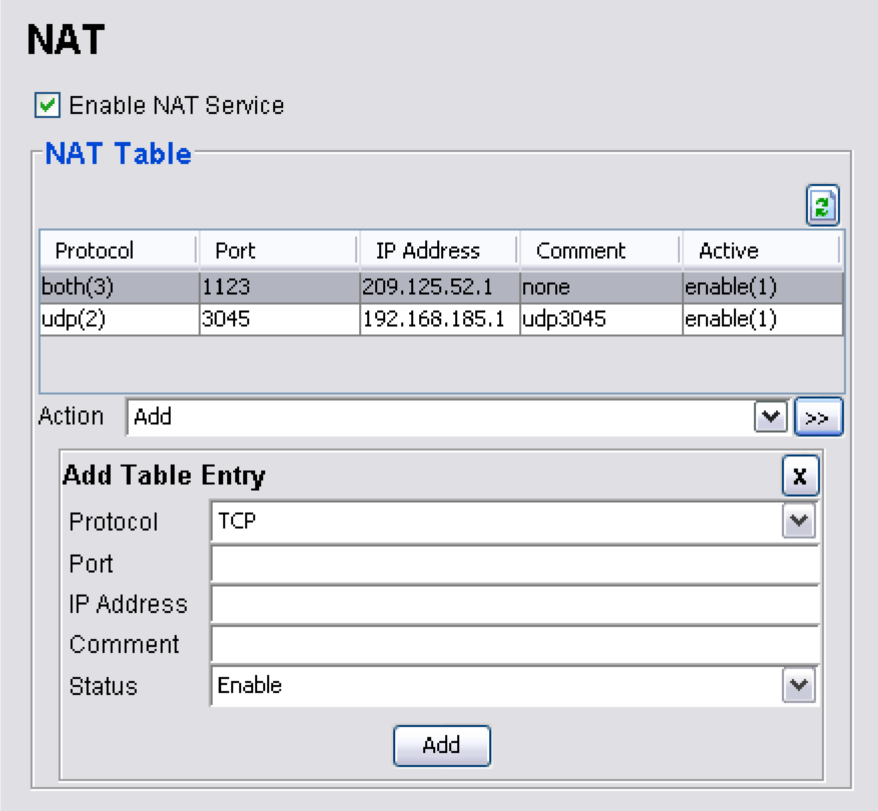
Mac Address	IP Address
00 6b 1c 91 0f e2	10.16.1.157
00 b5 02 88 f6 72	10.16.1.142

Add User to MAC Access Table

Allow

5.3.1.16 Services > NAT

The Network Address Translation service enables the clients with IP addresses that are not globally unique to connect to the network by translating those addresses into a globally routable IP address space.



NAT

☑ Enable NAT Service

NAT Table

Protocol	Port	IP Address	Comment	Active
both(3)	1123	209.125.52.1	none	enable(1)
udp(2)	3045	192.168.185.1	udp3045	enable(1)

Action: Add

Add Table Entry

Protocol	TCP
Port	
IP Address	
Comment	
Status	Enable

<u>Parameters</u>

1) Enable NAT Service
   - A checkbox to enable or disable the NAT service

<u>Parameters (NAT Table column)</u>

1) Protocol
   - Protocol to use. Choose from UDP, TCP and Both

2) Port
   - The port number to forward to.
   - Data type: Integer, in the range of 1 to 65535

3) IP Address
   - The destination host IP Address
   - Data type: IP Address

4) Comment

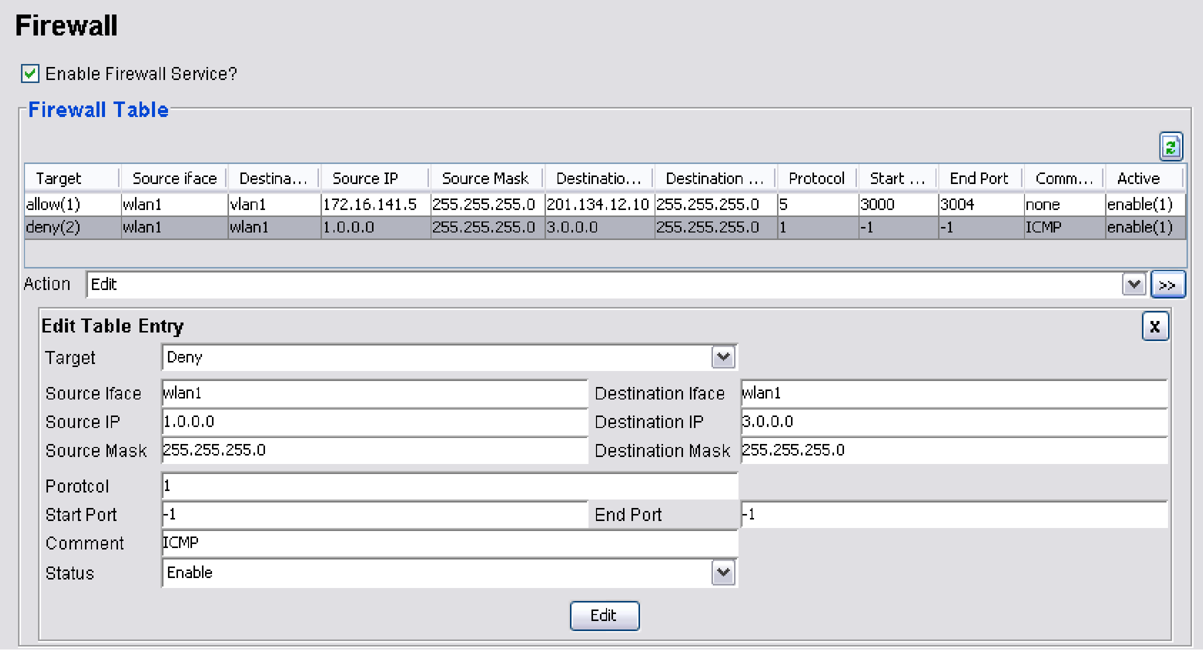
- An optional comment regarding the selected table entry
- Data type: Display String

5) Active

- The status of the selected table entry, either active or inactive

5.3.1.17 Services > Firewall

The Firewall service is the security feature that included in the Mesh AP to limit certain type of traffic. User can define and add a firewall rule through this configuration page.



Firewall

☑ Enable Firewall Service?

Firewall Table

Target	Source iface	Destina...	Source IP	Source Mask	Destinatio...	Destination ...	Protocol	Start ...	End Port	Comm...	Active
allow(1)	wlan1	vlan1	172.16.141.5	255.255.255.0	201.134.12.10	255.255.255.0	5	3000	3004	none	enable(1)
deny(2)	wlan1	wlan1	1.0.0.0	255.255.255.0	3.0.0.0	255.255.255.0	1	-1	-1	ICMP	enable(1)

Action: Edit

Edit Table Entry

Target	Deny		
Source Iface	wlan1	Destination Iface	wlan1
Source IP	1.0.0.0	Destination IP	3.0.0.0
Source Mask	255.255.255.0	Destination Mask	255.255.255.0
Porotcol	1		
Start Port	-1	End Port	-1
Comment	ICMP		
Status	Enable		

Parameter

1) Enable Firewall Service

- A checkbox to enable or disable the firewall service

Parameters (Firewall Table columns)

1) Target

- Define the type of the firewall rule, allow or deny the traffic

2) Source Iface

- The source interface of the firewall rule.
- Data type: Octet String

3) Destination Iface
   - The destination interface of the firewall rule
   - Data type: Octet String

4) Source IP & Mask
   - The IP Address and its netmask of the source interface
   - Data type: IP Address

5) Destination IP & Mask
   - The IP Address and its netmask of the destination interface
   - Data type: IP Address

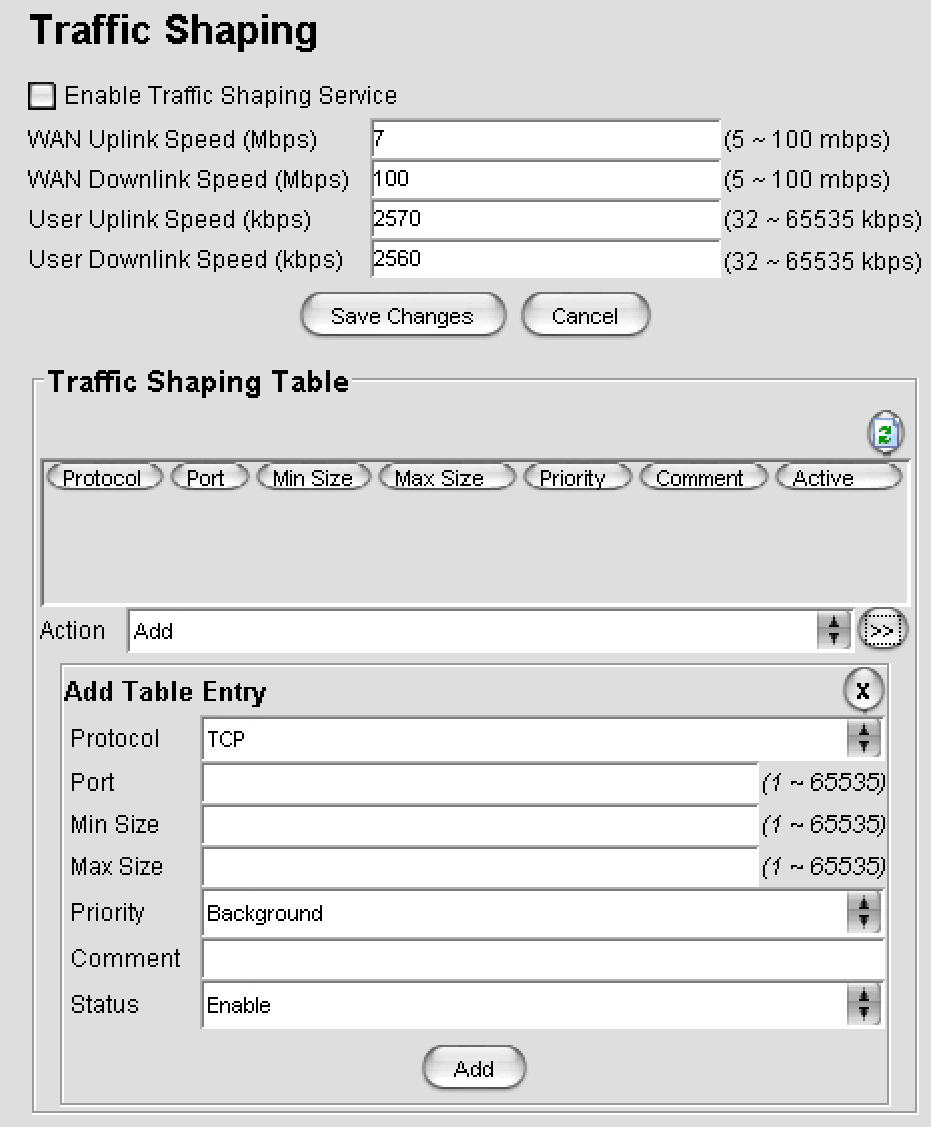
6) Protocol
   - The protocol of the rule.
   - Data type: Integer, in the range of 0 to 255

7) Start Port & End Port
   - The start and end define the range of port.
   - Data type: Integer, in the range of -1 to 65535
   - Fill the fields with '-1' if the ports is not applicable

8) Comment
   - An optional comment regarding the firewall rule
   - Data type: Display String

9) Active
   - The status of the firewall rule, either active or inactive

5.3.1.18 Services > Traffic Shaping



Traffic Shaping

□ Enable Traffic Shaping Service

WAN Uplink Speed (Mbps)	7	(5 ~ 100 mbps)
WAN Downlink Speed (Mbps)	100	(5 ~ 100 mbps)
User Uplink Speed (kbps)	2570	(32 ~ 65535 kbps)
User Downlink Speed (kbps)	2560	(32 ~ 65535 kbps)

Traffic Shaping Table

Protocol	Port	Min Size	Max Size	Priority	Comment	Active

Action: Add

Add Table Entry

Protocol	TCP	
Port		(1 ~ 65535)
Min Size		(1 ~ 65535)
Max Size		(1 ~ 65535)
Priority	Background	
Comment		
Status	Enable	

User can set the download and upload speed at the Traffic Shaping configuration page in order to alter the network performance. The Traffic Shaping Table defines the traffic volume for a port with a specified protocol.

<u>Parameters</u>

1) Enable Traffic Shaping service
   - A checkbox to enable or disable the Traffic Shaping service on the Mesh AP

2) WAN Uplink Speed
   - Define the upload speed of the WAN interface
   - Data type: Integer, in the range of 5 and 100 Mbps

3) WAN Downlink Speed
    - Define the download speed of the WAN interface
    - Data type: Integer, in the range of 5 and 100 Mbps

4) User Uplink Speed
    - Define the user default upload speed.
    - Data type: Integer, in the range of 32 and 65535 kbps

5) User Downlink Speed
    - Define the user default download speed
    - Data type: Integer, in the range of 32 and 65535 kbps

Parameters (Traffic Shaping Table)

1) Protocol
    - The protocol to use.
    - Available choice: UDP, TCP and Both

2) Port
    - The port number
    - Data type: Integer, in the range of 1 and 65535

3) Min Size
    - The minimum size of the data packet
    - Data type: Integer, in the range of 1 and 65535

4) Max Size
    - The maximum size of the data packet
    - Data type: Integer. in the range of 1 and 65535

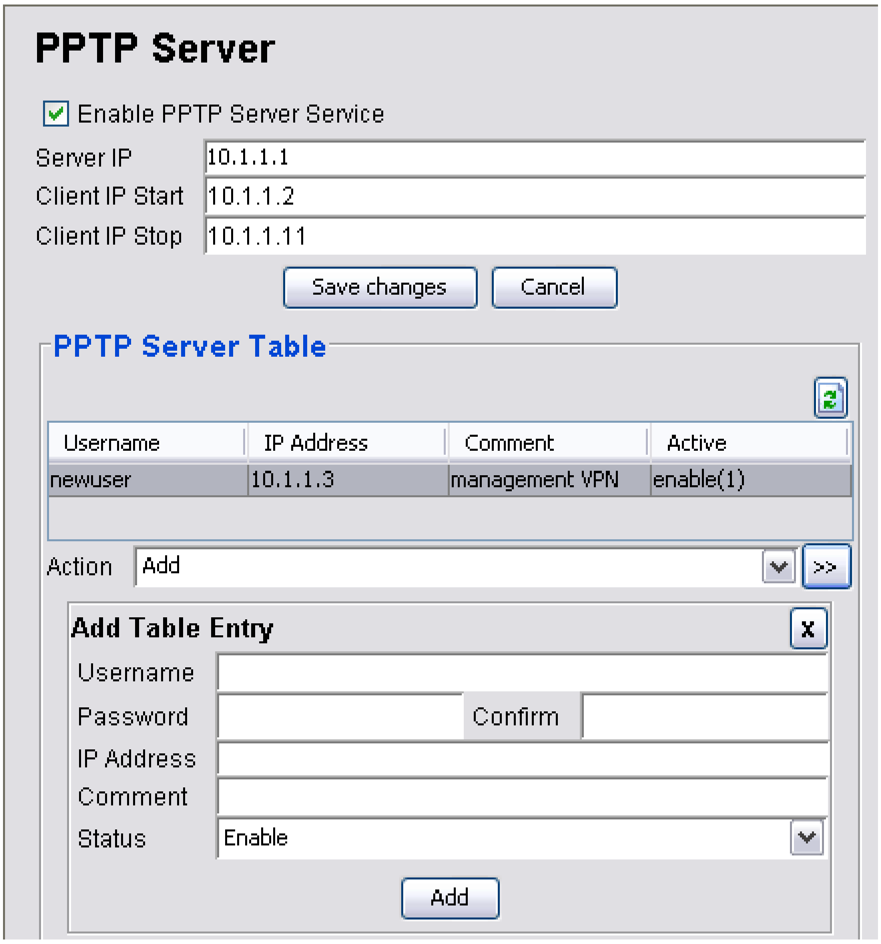
5) Priority
    - The priority to be assigned to the rule
    - Available choice: Background, Video, Voice and Best Effort

6) Comment
    - An optional comment regarding the table entry
    - Data type: Display String

7) Status

- The status of the table entry, either active or inactive

5.3.1.19 Services > PPTP Server



PPTP Server

☑ Enable PPTP Server Service

Server IP	10.1.1.1
Client IP Start	10.1.1.2
Client IP Stop	10.1.1.11

PPTP Server Table

Username	IP Address	Comment	Active
newuser	10.1.1.3	management VPN	enable(1)

Action: Add

Add Table Entry

Username			
Password		Confirm	
IP Address			
Comment			
Status	Enable		

The Point-to-Point Tunneling Protocol is best suits for remote access applications of VPNs. The PLANET Mesh Network Management Tools required a VPN connection to monitor the mesh network remotely. Hence a PPTP server is required. The PPTP Server is used to assign a user to a specified IP Address.

<u>Parameters:</u>

1) Enable PPTP Server Service
    - A checkbox to enable or disable the PPTP server service.

2) Server IP
    - The IP Address of the PPTP Server
    - Data type: IP Address

3) Client IP Start
    - The start of IP Address range assigned for the client
    - Data type: IP Address

4) Client IP Stop
    - The end of IP Address range assigned for the client
    - Data type: IP Address

Parameters (PPTP Server Table)

1) Username
    - The user name for the VPN client
    - Data type: Display String

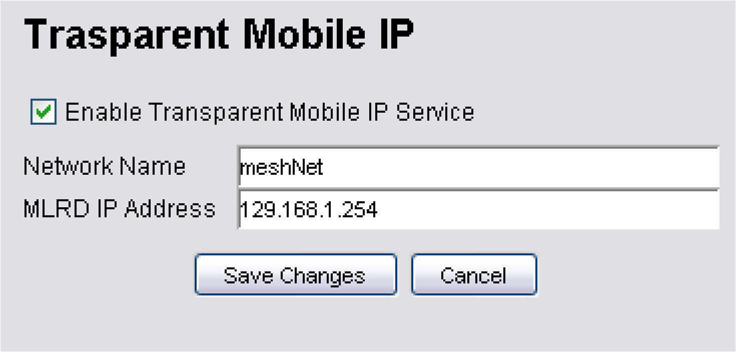
2) Password
    - The password corresponds to the username
    - Must re-enter the same password at the Confirm field.
    - Data type: Display String

3) IP Address
    - The IP Address assigned to the client
    - The IP MUST be in the range of the Client IPs pre-defined
    - Data type: IP Address

4) Comment
    - An optional comment regarding the PPTP client.
    - Data type: Display String

5) Active
    - Define the status of the PPTP Server table entry, either active or inactive

5.3.1.20 Services > Mobile IP (Future Feature)



Trasparent Mobile IP

☑ Enable Transparent Mobile IP Service

Network Name: meshNet

MLRD IP Address: 129.168.1.254

The Transparent Mobile IP is a feature that allows the AP's client, whose IP address is associated with one network, to stay connected when move on to another network with a different IP address. This feature proved advantage for the mobile device user who is not stationary.

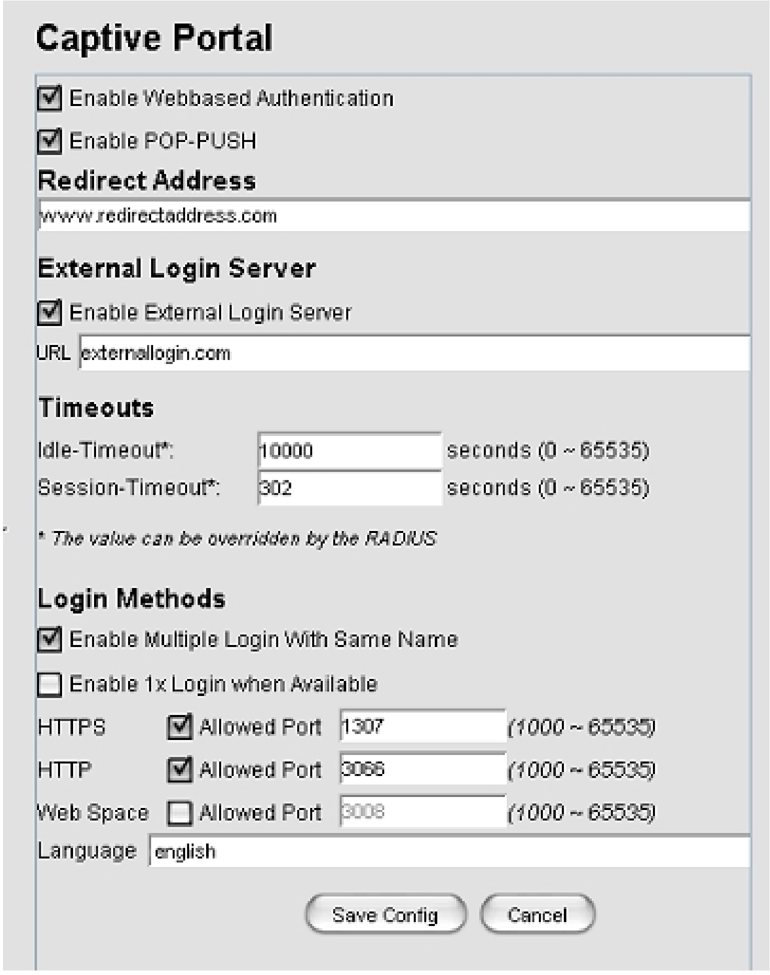
Parameters

1) Enable Transparent Mobile IP service
   - A checkbox to enable or disable the service of Mobile IP

2) Network Name
   - The Mobile IP community
   - Data type: Octet String

3) MLRD IP Address
   - The IP Address for the Mobile Location Register Daemon.
   - Data type: IP Address

5.3.1.21 Services > Captive Portal



Captive Portal

☑ Enable Webbased Authentication

☑ Enable POP-PUSH

Redirect Address

www.redirectaddress.com

External Login Server

☑ Enable External Login Server

URL externallogin.com

Timeouts

Idle-Timeout*: 10000 seconds (0 ~ 65535)

Session-Timeout*: 302 seconds (0 ~ 65535)

** The value can be overridden by the RADIUS*

Login Methods

☑ Enable Multiple Login With Same Name

□ Enable 1x Login when Available

HTTPS ☑ Allowed Port 1307 *(1000 ~ 65535)*

HTTP ☑ Allowed Port 3066 *(1000 ~ 65535)*

Web Space □ Allowed Port 3008 *(1000 ~ 65535)*

Language english

The Captive Portal configuration page defines the login parameter for a client user.

Parameters:

1) Enable Web-Based Authentication
   - A checkbox to enable or disable the Web-based authentication option

2) Enable POP-PUSH
   - A checkbox to enable or disable the feature of pushing email to unauthenticated users

3) Redirect Address
   - Define the URL where the user will be redirected to upon their successful login
   - Data type: Display String

4) Enable External Login Server
    - A checkbox to enable or disable the external login server

5) URL
    - The URL of the external login server
    - Data type: Display String

6) Idle-Timeout
    - The default value of time to wait, in seconds, before declaring the user is in the idle mode.
    - Data type: Integer, in the range of 1 and 65535

7) Session Timeout
    - The default value of time to wait, in seconds, before the session timeout
    - Data type: Integer, in the range of 1 and 65535

8) HTTPS allowed & Port
    - Tick the checkbox to enable user login with HTTPS.
    - Enabling the HTTPS will enable its correspond Port field, where to enter the HTTPS port number
    - Data type (Port): Integer, default value is 3000
    - Data range: 1000 ~ 65535

9) HTTP allowed & Port
    - Tick the checkbox to enable user login with HTTP
    - Enabling the HTTP will enable its correspond Port field, where to enter the HTTP port number
    - Data type (Port): Integer, default value is 3001
    - Data range: 1000 ~ 65535

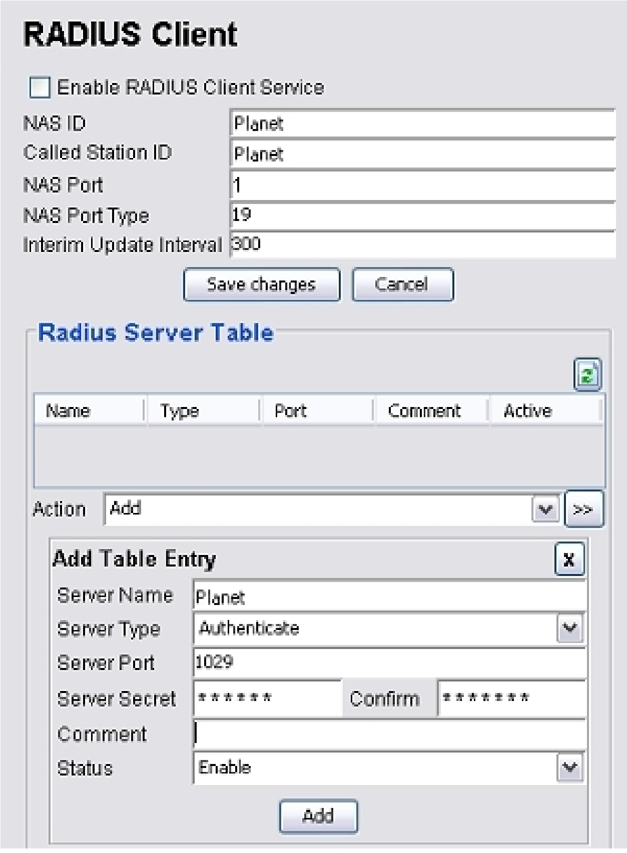
10) Web Space allowed & Port
    - Tick the checkbox to enable the internal web space.
    - Enabling the Web Space will enable its correspond Port field, where to enter the Web Space port number
    - Data type (Port): Integer, default value is 3003
    - Data range: 1000 ~ 65535

11) Language

- The login language: English

5.3.1.22 Services > Radius

The RADIUS server is used to authenticate and store the details of the client who log on to it. It also used as an accounting protocol for carrying accounting information between the network access server and a shared accounting server.



RADIUS Client

☐ Enable RADIUS Client Service

NAS ID	Planet
Called Station ID	Planet
NAS Port	1
NAS Port Type	19
Interim Update Interval	300

Radius Server Table

Name	Type	Port	Comment	Active

Action: Add

Add Table Entry

Server Name	Planet
Server Type	Authenticate
Server Port	1029
Server Secret	****** Confirm *******
Comment	
Status	Enable

Parameters

1) Enable RADIUS Client Service
   - A checkbox to enable or disable the RADIUS Client service

2) NAS ID
   - The NAS Identifier is a string that use to identify the NAS originating the Access-Request
   - Data type: Display String

3) Called Station ID
   - The called station ID allows the NAS to send in the Access-Request packet the phone number that the user called
   - Data type: Display String

4) NAS Port
   - The physical port number of the NAS, which is authentication the user
   - Data type: Integer, in the range of 1 and 65535

5) NAS Port Type
   - The NAS Port type defines the type of the physical port of the NAS, which is authenticating the user.
   - It can be used instead of, or in addition to the NAS Port field
   - Data type: Integer, in the range of 1 and 65535

6) Interim Update Interval
   - This field specifies the update interval, in seconds, for RADIUS accounting purpose.
   - Data type: Integer, in the range of 1 and 65535

Parameters (Radius Server Table column)

1) Server Name
   - The name of the RADIUS client
   - Data type: Display String

2) Server Type
   - The type of the server, which could be Accounting or Authentication

3) Server Port
   - The server port used by the client
   - Data type: Integer, in the range of 1 and 65535

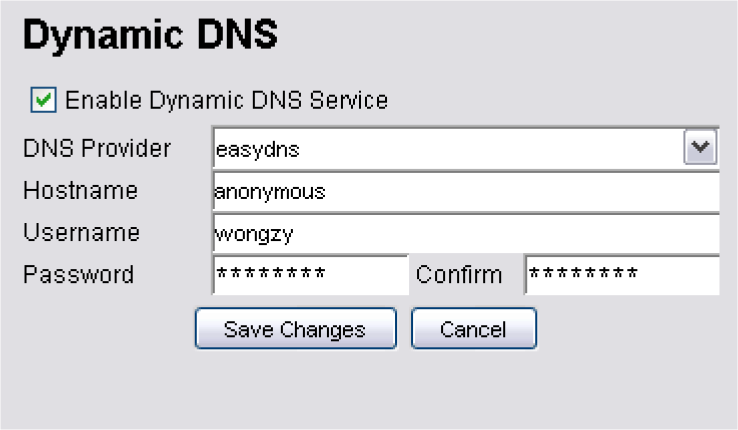
4) Server Secret
   - The client's secret key
   - MUST reenter the same secret key at the Confirm field.
   - Data type: Display String

5) Comment
   - An optional comment regarding the RADIUS client
   - Data type: Display String

6) Status

- Define the status of the table entry, either active or inactive

5.3.1.23 Services > Dynamic DNS



Dynamic DNS

☑ Enable Dynamic DNS Service

DNS Provider: easydns

Hostname: anonymous

Username: wongzy

Password: ******** Confirm: ********

The Dynamic DNS feature of the Mesh AP unit provides the ability to assign and tie the domain name to a dynamic IP Address. Hence, management from the other site of the network is able to connect to the device without tracing its IP Address. The page is used to configure the Dynamic DNS settings.

Parameter

1) Enable Dynamic DNS Service
   - A checkbox to enable or disable the feature of A checkbox to enable or disable the feature of Dynamic DNS

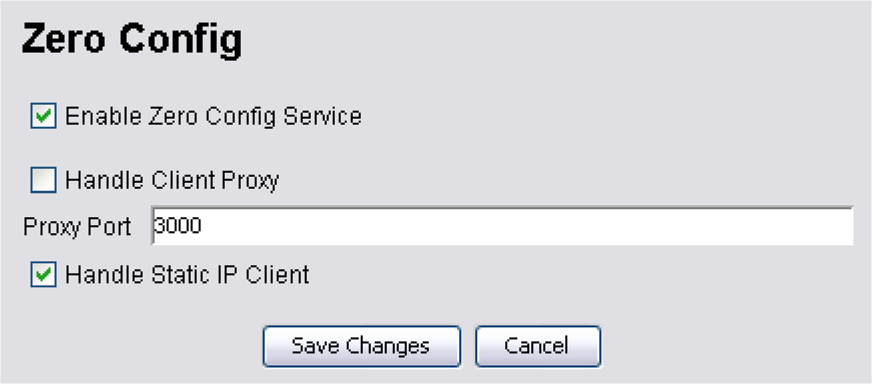
2) DNS Provider
   - Select the dynamic DNS provider
   - Available options: dyndns, easydns, no-ip, zoneedit, tzo

3) Hostname
   - The hostname associated with the service provider
   - Data type: Display String

4) Username
   - The username for the dynamic DNS service
   - Data type: Display String

5) Password
   - The password for the username above
   - Data type: Display String

5.3.1.24 Services > Zero Config



Zero Config

☑ Enable Zero Config Service

□ Handle Client Proxy

Proxy Port 3000

☑ Handle Static IP Client

<u>Parameters</u>

1) Enable Zero Config Service
   - A checkbox to enable or disable the Zero Config service of the Mesh AP

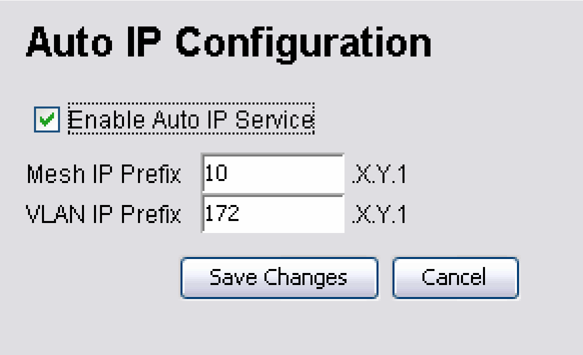
2) Handle Client Proxy
   - A checkbox to enable or disable the feature to handle client proxy

3) Proxy Port
   - The port used in proxy login
   - Data type: Integer, default value is 3001
   - Data range: 1000 ~ 65535

4) Handle Static IP Client
   - A checkbox to enable or disable the feature to handle static IP client

5.3.1.25 Services > Auto IP

The Auto IP Service of the system will assign a unique IP Address to the system. Upon the successful assignment, a Mesh IP Address and VLAN0 IP Address will be provided. As a result, the DHCPD settings will be altered to match with the VLAN0 IP.



Auto IP Configuration

☑ Enable Auto IP Service

Mesh IP Prefix 10 .X.Y.1

VLAN IP Prefix 172 .X.Y.1

Parameters

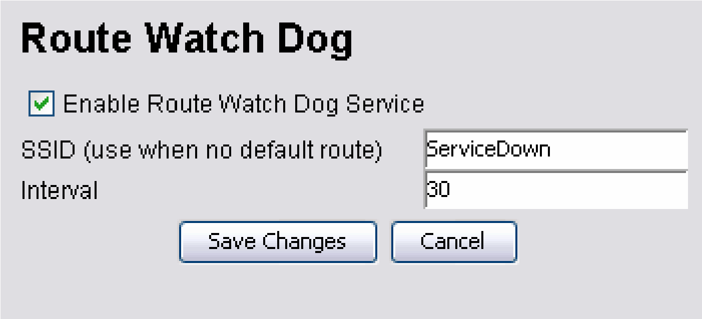
1) Enable Auto IP Service
    - A checkbox to enable or disable the Auto IP service of the Mesh AP

2) Mesh IP Prefix
    - Define the prefix of the Mesh IP Address.
    - Data Type: Integer, in the range of 0 to 255
    - Default Value: 10

3) VLAN IP Prefix
    - Define the prefix of the VLAN0 IP Address
    - Data type: Integer, in the range of 0 to 255
    - Default value is 172

5.3.1.26 Services -> Route Watch Dog

The route watchdog will probe for default route periodically. In case if the default route is not detected, it will change the ESSID of the active wireless radio to the value set in this panel, as to alert the user regarding the failure.



Route Watch Dog

☑ Enable Route Watch Dog Service

SSID (use when no default route): ServiceDown

Interval: 30

Parameters

1) Enable Route Watch Dog Service
    - A checkbox to enable or disable the route watchdog service of the Mesh AP unit

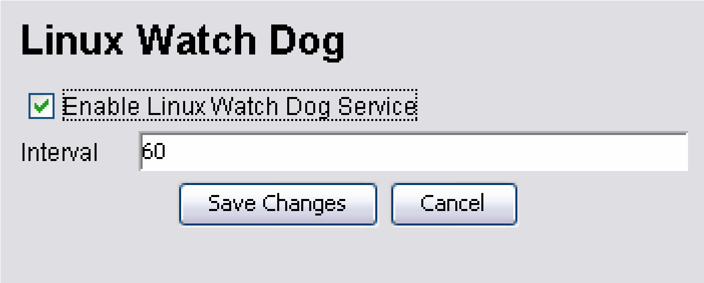
2) SSID
    - The SSID used when the default route is not detected throughout the watchdog routine.
    - Data Type: Display String

3) Interval

- The checking interval of the route watch dog, in seconds
- Data Type: Integer, in the range of 10 to 60
- Default value: 30

5.3.1.27 Services -> System Watch Dog

The Linux kernel watchdog is intended to monitor the integrity of the system periodically. In case if there is any error occurs, the watch dog would trigger a system reboot in order to prevent the system from failure.



Linux Watch Dog

☑ Enable Linux Watch Dog Service

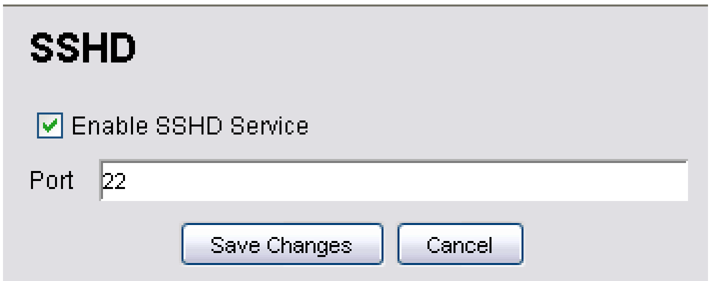
Interval: 60

Parameters

1) Enable Linux Watch Dog Service
   - A checkbox to enable or disable the route watchdog service of the Mesh AP unit

2) Interval
   - The checking interval of the linux kernel watch dog, in seconds
   - Data Type: Integer, in the range of 10 to 60 seconds
   - Default value: 60

5.3.1.28 Services -> SSHD



SSHD

☑ Enable SSHD Service

Port: 22

At this page user will configure the SSH feature of the device.

Parameters

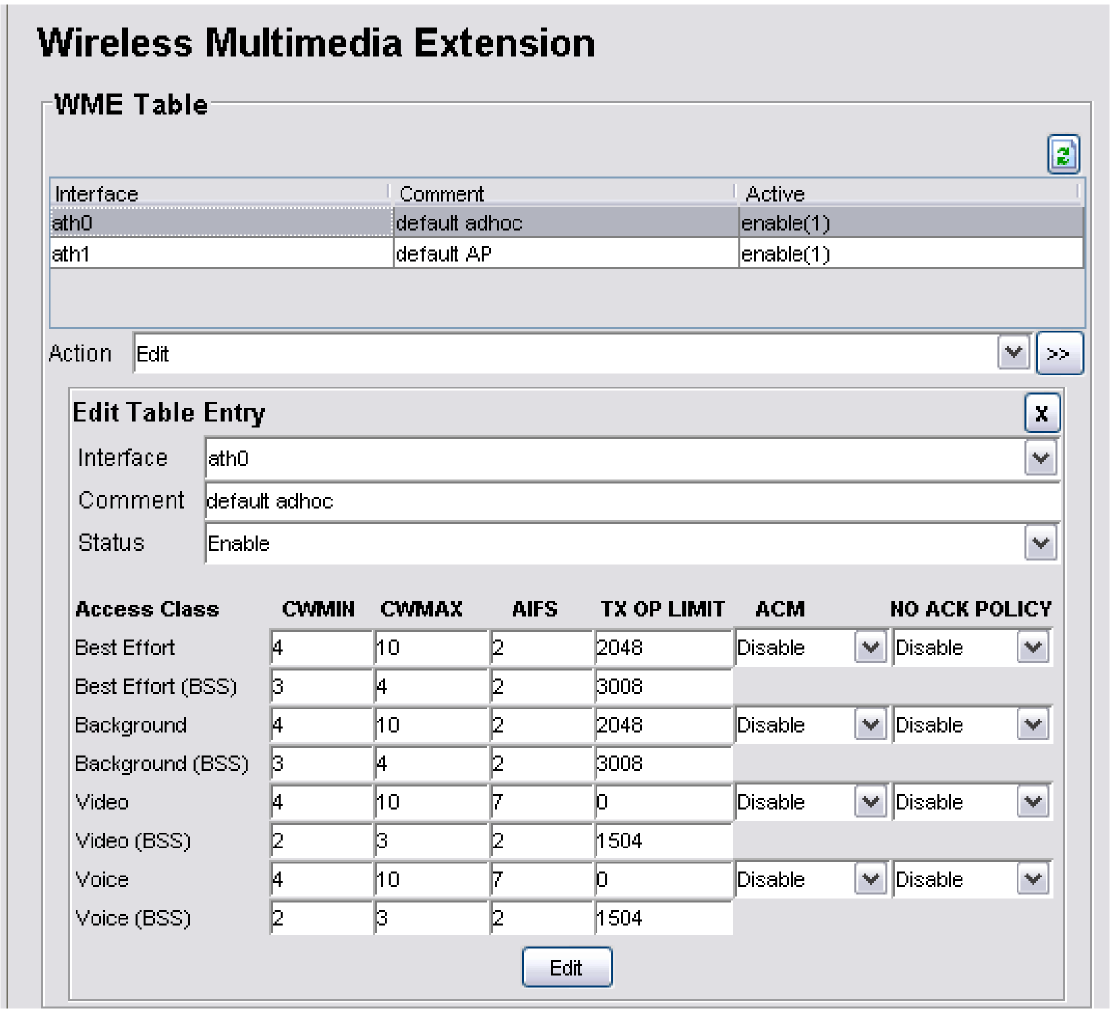
1) Enable SSHD Service
   - A checkbox to enable or disable the SSH service of the Mesh AP unit

2) Port

- The port number to be used by the SSH service
- Data Type: Integer, in the range of 1 and 65535
- Default value: 22

5.3.1.29 Services > WME

This page allows administrator to define the wifi multimedia QoS settings for each wireless interface. WME defines eight categories: best effort, background, video and voice, with and without BSS (Basic Service Set) mode.



Wireless Multimedia Extension

WME Table

Interface	Comment	Active
ath0	default adhoc	enable(1)
ath1	default AP	enable(1)

Action: Edit

Edit Table Entry

Interface: ath0

Comment: default adhoc

Status: Enable

Access Class	CWMIN	CWMAX	AIFS	TX OP LIMIT	ACM	NO ACK POLICY
Best Effort	4	10	2	2048	Disable	Disable
Best Effort (BSS)	3	4	2	3008		
Background	4	10	2	2048	Disable	Disable
Background (BSS)	3	4	2	3008		
Video	4	10	7	0	Disable	Disable
Video (BSS)	2	3	2	1504		
Voice	4	10	7	0	Disable	Disable
Voice (BSS)	2	3	2	1504		

Parameters (WMM Table)

1) Interface

- The available wireless interfaces in the system

2) CWMIN

- CW defines the contention window size, which is the dynamic backoff interval for legacy DCP implementation.
- CWMIN specifies the minimum of CW value, in milliseconds
- Apply to all eight classes
- Data type: Integer, in the range of 0 to 255

3) CWMAX
   - The maximum of CW value, in milliseconds
   - Apply to all eight classes
   - Data type: Integer, in the range of 0 to 255

4) AIFS
   - AIFS specifies the time interval between medium-idle and the start of media access negotiations, in milliseconds
   - Apply to all eight classes
   - Data type: Integer, in the range of 0 to 255

5) TX OP LIMIT
   - TXOPLIMIT (Transmit Opportunity Limit) specifies the duration that an end-user device can transmit for the specific access category, in milliseconds
   - Apply to all eight classes
   - Data type: Integer, in the range of 0 to 65535

6) ACM
   - Enable of disable the admission control for the access classes that without BSS

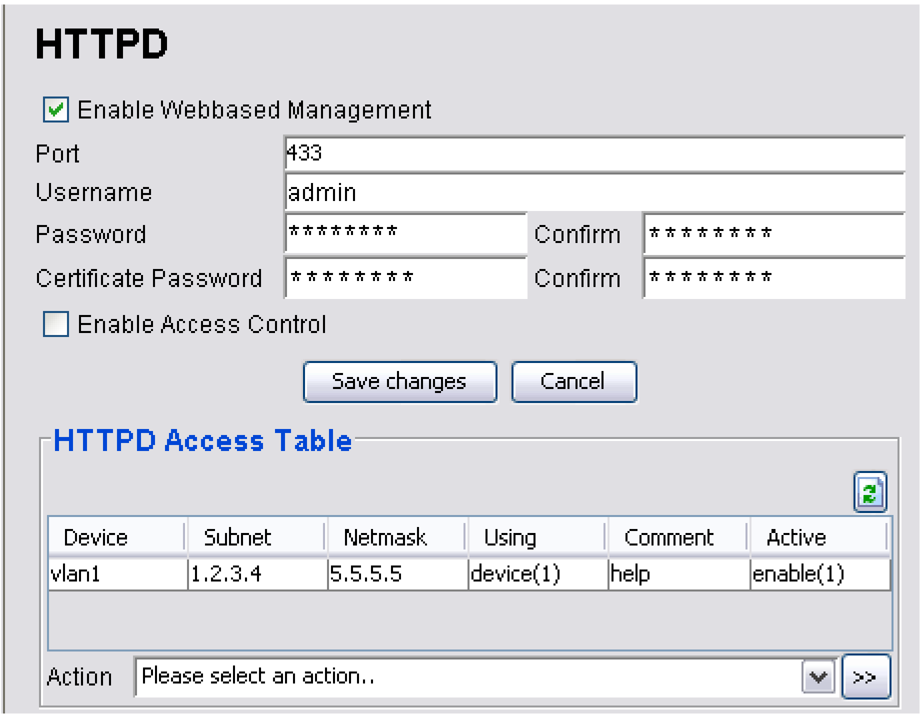
7) NO ACK POLICY
   - Enable of disable the support of no-ack for the access categories that without BSS

8) Comment
   - An optional comment regarding the table entry

9) Status
   - Enable or Disable this table entry.

5.3.1.30 Management > HTTPD

The HTTPD configuration page is to alter the settings on the Web-based management. The HTTPD Access Table in this page defines the access control of the HTTPD management.



HTTPD

☑ Enable Webbased Management

Port	433		
Username	admin		
Password	********	Confirm	********
Certificate Password	********	Confirm	********

□ Enable Access Control

HTTPD Access Table

Device	Subnet	Netmask	Using	Comment	Active
vlan1	1.2.3.4	5.5.5.5	device(1)	help	enable(1)

Action: Please select an action..

Parameters:

1) Enable Webbased Management

- A checkbox to enable or disable Web-based management of the Mesh AP unit

2) Port

- The field defines the port used for HTTP daemon
- Data type: Integer, default value is 443
- Data range: 1 ~ 65535

3) Username

- The username of the HTTP admin
- Data type: Display String, default value is “admin”

4) Password

- The password corresponding to the username above
- Data type: Display String, default value is “admin”

5) Certificate Password
    - The password for the HTTP certificate
    - Data type: Display String, default value is “httpconf”

6) Enable Access Control
    - A checkbox to enable or disable the access control of the HTTP daemon.

<u>Parameters (HTTPD Access Table)</u>

1) Device
    - The name of the device allowed for access control
    - Data type: Octet String

2) Subnet
    - The subnet allowed for access control
    - Data type: IP Address

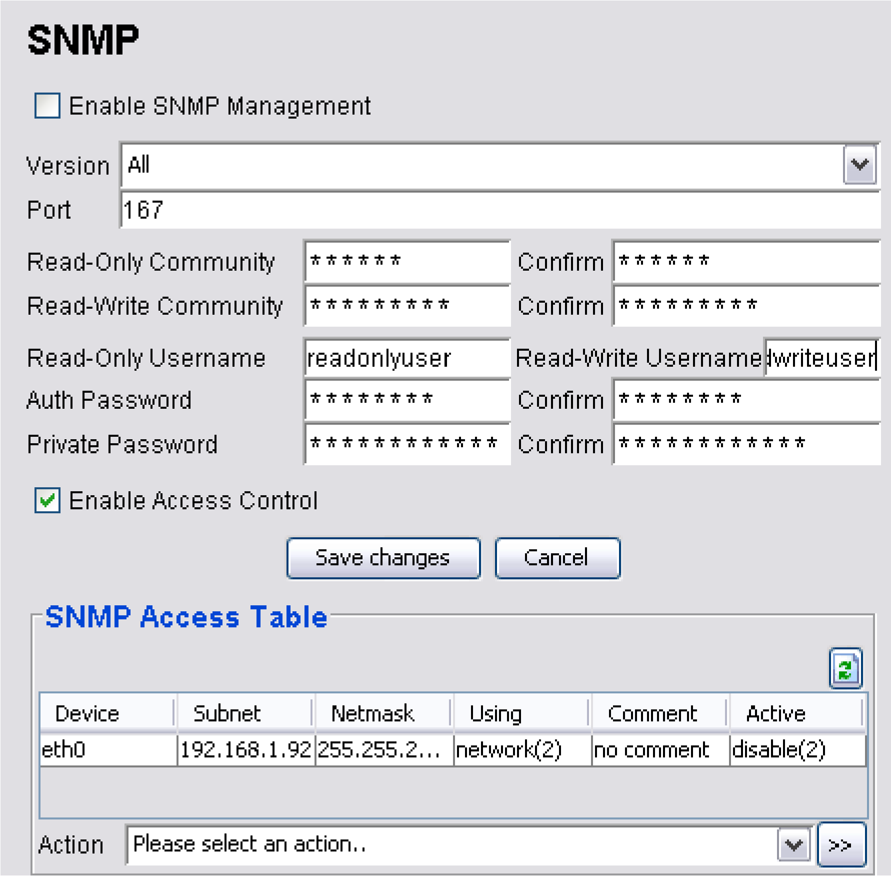
3) Netmask
    - The netmask for the Subnet IP above
    - Data type: IP Address

4) Using
    - Define the type of access control to use through, either Device or Subnet

5) Comment
    - An optional comment regarding the table entry
    - Data type: Display String

6) Active
    - Define the status of the table entry, either active or inactive

5.3.1.31 Management > SNMPD



SNMP

□ Enable SNMP Management

Version: All

Port: 167

Read-Only Community: ****** Confirm: ******

Read-Write Community: ********* Confirm: *********

Read-Only Username: readonlyuser Read-Write Username: writeuser

Auth Password: ******** Confirm: ********

Private Password: ************ Confirm: ************

☑ Enable Access Control

SNMP Access Table

Device	Subnet	Netmask	Using	Comment	Active
eth0	192.168.1.92	255.255.2...	network(2)	no comment	disable(2)

Action: Please select an action..

This configuration page is used to alter the setting of the SNMP daemon in the Mesh AP unit. The SNMP Access Table defines the access control of the SNMP management.

<u>Parameters</u>

1) Enable SNMP Management
   - A checkbox to enable or disable the SNMP management
2) Version
   - Define the SNMP version to use.
   - Available selection: Version 1 or 2c, Version 3 and All

3) Port
   - This field specifies the port used for SNMP management
   - Data type: Integer, default is 161

4) Read-Only Community
   - The community keyword used for SNMP version 1 or 2c, which allow the read accessing only.

- Data type: Display String, default value is “public”
- Data length: 4 ~ 32
- MUST reenter the same community at the correspond Confirm field to edit
- Please retain this parameters as it is used to plot the topology map

5) Read-Write Community
    - The community keyword used for SNMP version 1 or 2c, which allow both the read and write accessing
    - Data type: Display String, default value is “private”
    - Data length: 4 ~ 32
    - MUST reenter the same community at the correspond Confirm field to edit

6) Read-Only Username
    - The principal name of the SNMP version 3 daemon, which allow the read accessing only
    - Data type: Display String, default value is “snmpv3rouser”
    - Data length: 8 ~ 50

7) Read-Write Username
    - The principal name of the SNMP version 3 daemon, which allow both the read and write accessing
    - Data type: Display String, default value is “snmpv3rwuser”
    - Data length: 8 ~ 50

8) Auth Password
    - The password used user authentication (SNMP version 3 only)
    - Data type: Display String, default value is “snmpv3password”
    - Data length: 8 ~ 50
    - MUST reenter the same password at the correspond Confirm field

9) Privacy Password
    - The privacy protocol pass phrase used for SNMP version 3 only
    - Data type: Display String, default value is “snmpv3passphrase”
    - Data length: 8 ~ 50
    - MUST reenter the same password at the correspond Confirm field

10) Enable Access Control

- A checkbox to enable the access control of the SNMP daemon manangement

Parameters (SNMP Access Table)

1) Device
    - The name of the device allowed for access control
    - Data type: Octet String

2) Subnet
    - The subnet allowed for access control
    - Data type: IP Address

3) Netmask
    - The netmask for the Subnet IP above
    - Data type: IP Address

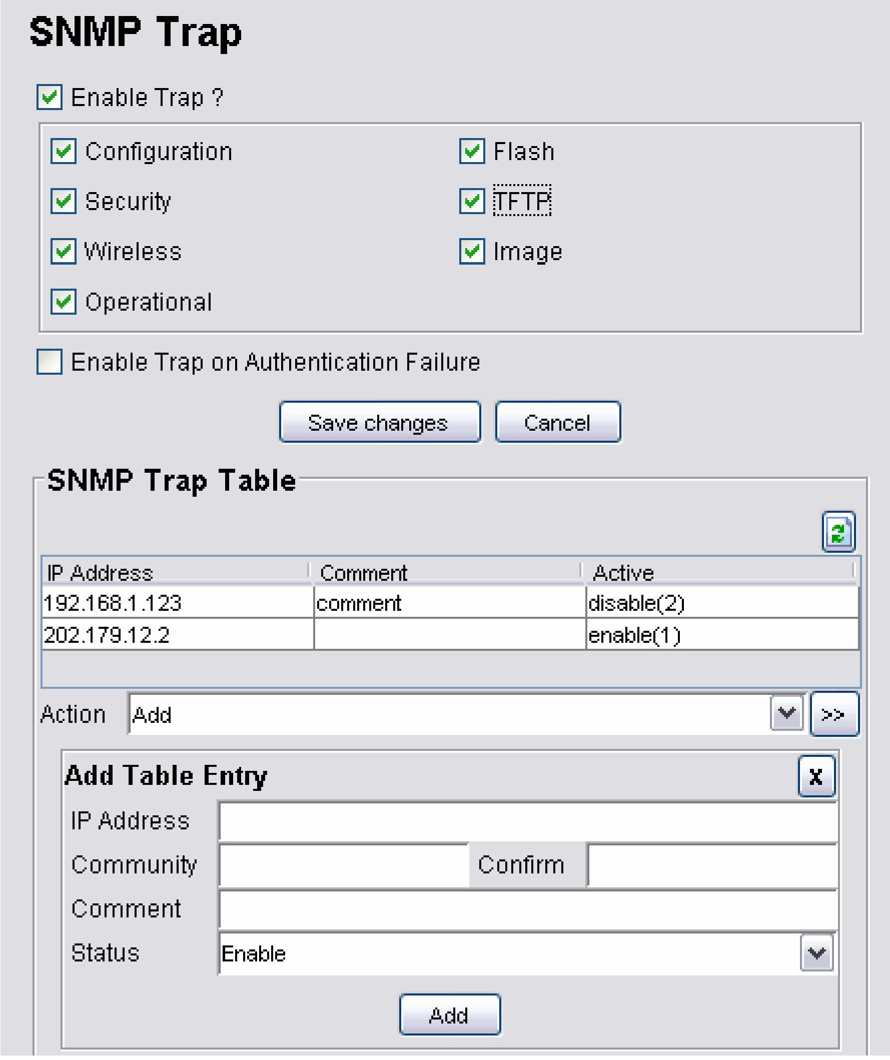
4) Using
    - Define the type of access control to use through, either Device or Subnet

5) Comment
    - An optional comment regarding the table entry
    - Data type: Display String

6) Active
    - Define the status of the table entry, either active or inactive

5.3.1.32 Management > SNMP Trap

The SNMP Alarm system embedded in the Mesh AP unit can be configured through this page. The SNMP Trap Table in this page lists the SNMP Trap hosts.



SNMP Trap

☑ Enable Trap ?

☑ Configuration ☑ Flash

☑ Security ☑ TFTP

☑ Wireless ☑ Image

☑ Operational

☐ Enable Trap on Authentication Failure

SNMP Trap Table

IP Address	Comment	Active
192.168.1.123	comment	disable(2)
202.179.12.2		enable(1)

Action: Add

Add Table Entry

IP Address			
Community		Confirm	
Comment			
Status	Enable		

Parameters:

1) Enable Trap

- A checkbox to enable or disable the SNMP trap feature

2) Configuration

- A checkbox to enable or disable the system to send the traps regarding configuration

3) Security

- A checkbox to enable or disable the system to send the security traps

4) Wireless

- A checkbox to enable or disable the system to send the traps regarding wireless

5) Operational
    - A checkbox to enable or disable the system to send the operational traps

6) Flash
    - A checkbox to enable or disable the system to send the traps regarding Flash

7) TFTP
    - A checkbox to enable or disable the system to send the traps regarding TFTP

8) Image
    - A checkbox to enable or disable the system to send the trap regarding Image

9) Enable Trap on Authentication Failure
    - A checkbox to enable or disable the trap on authentication failure

<u>Parameters (SNMP Trap Table)</u>

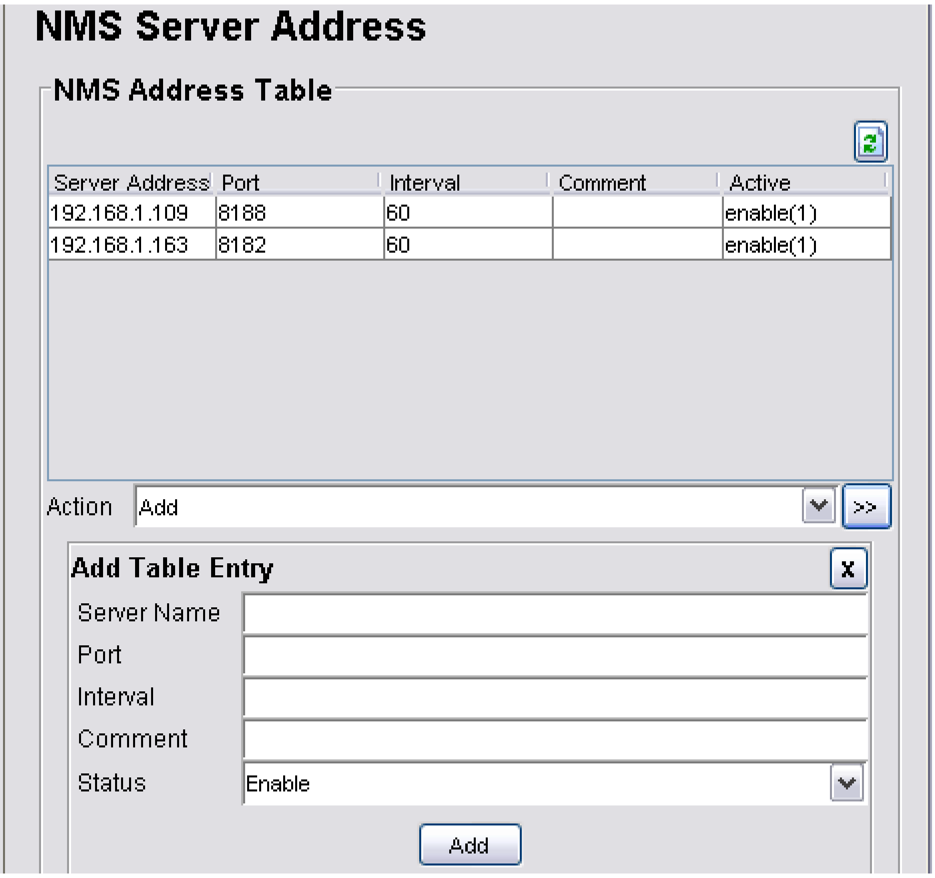
1) IP Address
    - The destination IP Address of the trap receiver, to receive the trap
    - Data type: IP Address

2) Community
    - The community keyword of the SNMP Trap.
    - Data type: Display String, default value is “public”
    - MUST reenter the same community at the correspond Confirm field

3) Comment
    - An optional comment regarding the table entry
    - Data type: Display String

4) Active
    - Define the status of the table entry, either active or inactive

5.3.1.33 Management > NMS Address



NMS Server Address

NMS Address Table

Server Address	Port	Interval	Comment	Active
192.168.1.109	8188	60		enable(1)
192.168.1.163	8182	60		enable(1)

Action: Add

Add Table Entry

Server Name	
Port	
Interval	
Comment	
Status	Enable

This table defines the destination of the notification. By adding a new entry, with the IP Address and port number of the NMS, into the table, the AP would redirect a notification to the specific NMS, in the defined interval. This table applies to every operating mode of the AP.

<u>Parameters (SNMP Trap Table)</u>

1) Server Name
   - The destination IP Address / DNS of the NMS Server, to receive the notification from this AP.
   - Data type: DisplayString

2) Port
   - The port number of the remote NMS to receive the notification
   - Data type: Integer, ranged from 1 to 65535, with default value 8188

3) Interval
   - The interval for the AP to send the notification message periodically, in seconds.
   - Data type: Integer, ranged from 60 to 300000, with default value 60

4) Comment

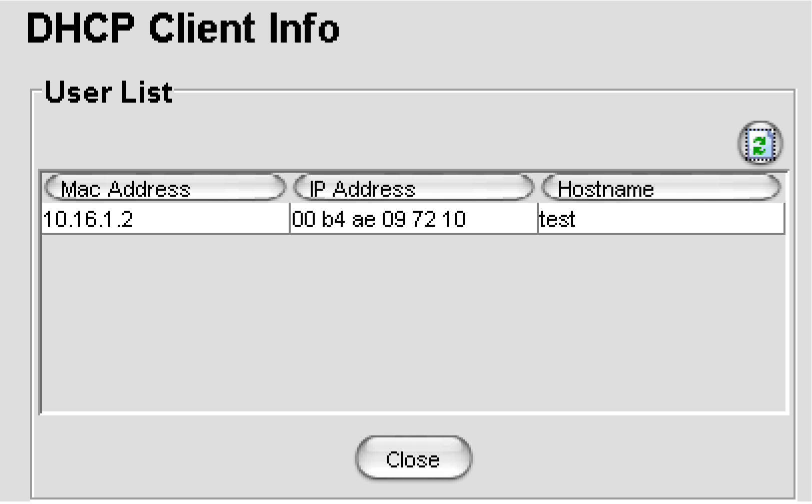
- An optional comment regarding the table entry
- Data type: Display String

5) Active

- Define the status of the table entry, either active or inactive

5.3.1.34 Status > DHCP Client

At the status tab, the DHCP Client list displays the DHCP Client information such as Mac Address, IP Address and their hostname. This table is a read-only table, hence administrator is unable to edit the table using the AP Configurator.

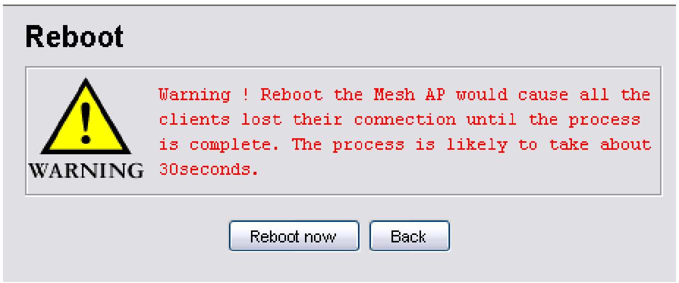


DHCP Client Info

User List

Mac Address	IP Address	Hostname
10.16.1.2	00 b4 ae 09 72 10	test

5.3.1.35 Command > Reboot



Reboot

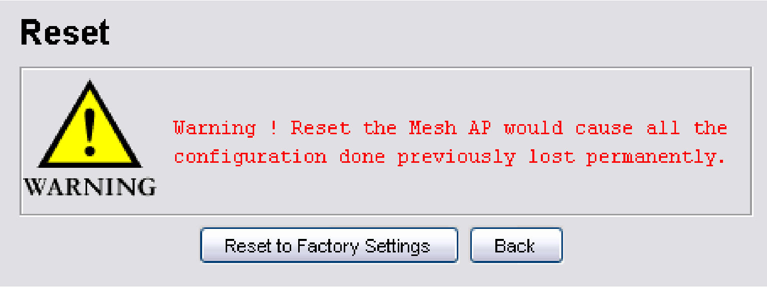
Warning ! Reboot the Mesh AP would cause all the clients lost their connection until the process is complete. The process is likely to take about 30seconds.

The reboot feature in the AP Configurator enables the NMS admin to restart the Mesh AP, thru the SNMP protocol, even if they are located remotely from the user. Once executed, all the service provided by the AP will be halted, until the reboot process completed successfully.

In order to reboot the Mesh AP, click on the **Reboot now** button in the Command > Reboot page, and confirm the process at the window popup.

Note that the changes that perform on the AP thru the AP Configurator required a reboot to commit to the device.

5.3.1.36 Command > Reset

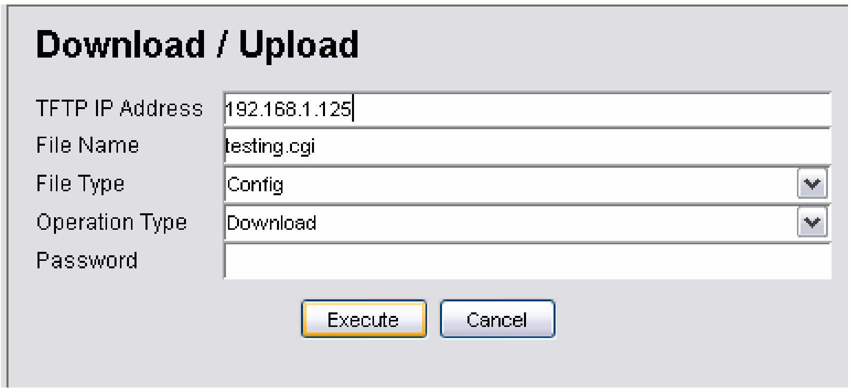

Reset

Warning ! Reset the Mesh AP would cause all the configuration done previously lost permanently.

The reset feature, meanwhile, provide the user of the NMS to restore the factory default parameters back to the device. This feature is extremely effective especially on the occasion where the Mesh AP is having some error due to inappropriate configuration. However please note that once the reset is performed, all the settings or changes done previously on the AP will be removed permanently.

In order to reset the Mesh AP, click on the **Reset to Factory Settings** button in the Command > Reset panel, and confirm the action at the popup window. Hit the **Back** button if you wish to cancel the command.

5.3.1.37 Command > Download/Upload


Download / Upload

TFTP IP Address	192.168.1.125
File Name	testing.cgi
File Type	Config
Operation Type	Download
Password	

This feature of the NMS enables the user to download or upload some files from or to the

Mesh AP unit via the TFTP protocol. By fill in the TFTP server IP address, the name of the file as well as its type, and then define the type of operation, hit the **Execute** button will do. Three types of operation are available, download, upload, and upload & reboot. Note that the operation type download is only available for file type Config. The Password field is to enter the key used for extract the IP x 509 local certificates.

6 Technical Support

For Technical Support and other related feedback and information request, kindly please send your request to the following email:

Email: support_wireless@planet.com.tw

In your email, please provide the following detail information:

Device Model No :

Distributor :

Date of Purchase :

Device MAC Address :

Brief Description of your Problem or Request :

Capture of Sys Log Info :

Contact Info

Name :

Company :

Email :